154157/EU XXV. GP
Eingelangt am 14/09/17

Council of the European Union

Brussels, 14 September 2017
(OR. en)

12181/17
ADD 1

Interinstitutional File:
2017/0226 (COD)

DROIPEN 120
CYBER 126
JAI 784
TELECOM 206
MI 626
IA 138
CODEC 1400

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	13 September 2017
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2017) 298 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

Delegations will find attached document SWD(2017) 298 final.

Encl.: SWD(2017) 298 final

www.parlament.gv.at

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 298 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

{COM(2017) 489 final}
{SWD(2017) 299 final}

www.parlament.gv.at

Contents

www.parlament.gv.at

www.parlament.gv.at

1. WHAT IS THE PROBLEM AND WHY IS IT A PROBLEM

1.1. Policy context

The Framework Decision

The current EU legislation that provides common minimum rules to criminalise non-cash payment fraud is the Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[1].

The Framework Decision was part of the first EU Fraud Prevention Action Plan 2001,[2] which aimed to improve the prevention of fraud and counterfeiting of non-cash payments, especially by extending the cooperation and exchange of information for investigation and prosecution between the competent authorities of the Member States and by boosting the fraud prevention measures.

The main components of the Framework Decision are:

- Definition of "payment instrument" as any physical ("corporeal") payment instrument which can be used to transfer money or monetary value and is protected against imitation or fraudulent use.
- Identification of different forms of behaviours requiring criminalisation in relation to fraud and counterfeiting of non-cash means of payments: offences related to payment instruments (e.g. theft, counterfeiting, falsification, receiving or selling fraudulent use stolen or counterfeited payment instruments, use of a stolen or counterfeited payment instrument); offences related to computers (i.e. performing or causing a transfer of money by introducing, altering, deleting or suppressing computer data or by interfering with the functioning of a computer programme or system); offences related to specifically adapted devices (e.g. fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsification of a payment instrument).
- Rules on liability and sanctions for legal persons, provisions on establishing jurisdiction on offences relating to non-cash payment fraud, on extradition and prosecution and rules to facilitate cross-border cooperation and exchange of information.

EU policy and legislative context

The policy and legislative context has significantly changed since the Framework Decision was adopted. Various legislative acts at EU level have been adopted since 2001, both in criminal and civil law, which:

[1] Official Journal L 149 , 02/06/2001 P. 0001 - 0004, referred to as the Framework Decision in this document
[2] Commission Communication "Preventing fraud and counterfeiting of non-cash means of payment", COM(2001) 11 final of 9.2.2001.

www.parlament.gv.at

1. provide pan-European **cooperation mechanisms in criminal matters** that facilitate coordination of investigation and prosecution (procedural criminal law). These include:
    - Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States[3] (EAW), which sets conditions for compulsory extradition for offences covered by the Framework Decision (e.g. “fraud, including that affecting the financial interests of the European Communities”, “forgery of means of payment”, “computer-related crime”, “participation in a criminal organisation”) when they are punished by a certain level of penalties. Member States can no longer refuse to extradite to another Member State citizens on the sole grounds of nationality, in case the offences committed are punishable by a custodial sentence or a detention order for a maximum period of at least three years. The European Arrest Warrant may apply for offences punishable by imprisonment or a detention order for a maximum period of at least 1 year or where a final custodial sentence has been passed or a detention order has been made, for sentences of at least 4 months.
    - Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[4], which sets up the conditions when the mutual assistance shall be afforded.
    - Directive 2014/41/EU regarding the European Investigation Order in criminal matters[5], which updates the legal framework applicable to the gathering and transfer of evidence between Member States, based on mutual recognition of judicial decisions. It allows an authority in one Member State (the "issuing authority") to request specific criminal investigative measures be carried out by an authority in another Member State (the "executing authority").
    - Council Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties[6], which facilitates the enforcement of financial penalties in cross-border cases, wherever in the EU they may have been imposed. It abolishes dual criminality checks in relation to 39 listed offences, which include fraud as well as counterfeiting of currency.
    - Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings[7], which aims to improve judicial cooperation between Member States so as to prevent unnecessary parallel criminal proceedings concerning the same facts and the same person. It lays out the procedure whereby competent national authorities contact each other when they have reasonable grounds to believe that parallel

[3] 2002/584/JHA Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States
[4] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union
[5] Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters
[6] Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties
[7] Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings

proceedings are being conducted in another EU country. It also establishes the framework for these authorities to enter into direct consultations when parallel proceedings exist, in order to find a solution to avoid the negative consequences arising from these proceedings.

- Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States[8], which sets out the general principles for the functioning of the exchange of criminal records between EU countries, alongside Council Decision 2009/316/JHA on the establishment of the European Criminal Records Information System (ECRIS)[9] in application of Article 11 of Framework Decision 2009/315/JHA, which establishes ECRIS. They seek to prevent criminals from escaping their past by moving to a different EU country from that in which they were convicted. They do this by ensuring that information on all their convictions is available when needed, irrespective of the EU country in which they were convicted. They set an obligation for an EU country convicting a national of another EU country to transmit information on such conviction to the country of his nationality and define the obligations of the EU country of which the person is a national to store the received information on convictions as well as the procedures which that EU country is to follow when replying to requests for information about its nationals.
- Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime[10], which provides minimum standards on the rights, support and protection of victims of crime, ensuring that they receive appropriate information, support and protection and may participate in criminal proceedings wherever the damage occurred in the EU. These victims must have the right to, e.g., recover stolen property, have their expenses reimbursed, receive legal aid and have their case heard in court.
- Council conclusions on improving criminal justice in cyberspace[11], in which the Council called on the Commission to take concrete actions based on a common EU approach to improve cooperation with service providers, make mutual legal assistance more efficient and to propose solutions to the problems of determining and enforcing jurisdiction in cyberspace. In response to these conclusions, The Commission conducted an expert consultation process and summarized its results in a non-paper[12], presented to the Council on June 8 2017, which may result in a legislative initiative.

[8] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States
[9] Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA
[10] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
[11] Council conclusions of 6 June 2016 on improving criminal justice in cyberspace
[12] Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, June 2017

- Regulation (EU) 2016/794 on Europol[13], which sets up the rules for Europol, in particular its:
  - objectives, including mutual cooperation amongst EU countries in preventing and combating terrorism, serious crime affecting two or more EU countries and forms of crime which affect a common interest covered by EU policy;
  - tasks, including collecting, storing, processing, analysing and exchanging information including criminal intelligence, as well as coordinating, organising and implementing investigative and operational actions to support Member States and supporting EU countries in combating crime enabled, promoted or committed using the internet), and
  - scrutiny, including monitoring of Europol's processing of personal data.
- Council Decision 2002/187/JHA setting up Eurojust[14], which facilitates cross-border judicial cooperation in criminal matters.

2. **criminalise conduct** related to fraud and counterfeiting of non-cash means of payment (substantive criminal law). These include:
   - Directive 2013/40/EU on attacks against information systems[15], which establishes minimum rules concerning the definition of criminal offences and the relevant sanctions, and to improve cooperation between competent authorities.
   - Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law[16], which establishes minimum rules concerning the definition of criminal offences and sanctions, and introduces provisions to strengthen investigation of offences and cooperation against counterfeiting.
   - Directive 2017/541/EU on combating terrorism[17], which criminalises providing or collecting funds with the intention or the knowledge that they are to be used to commit terrorist offences and offences related to terrorist groups or terrorist activities.

[13] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

[14] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime

[15] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[16] Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA

[17] Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

- The Proposal for a Directive on countering money laundering by criminal law[18], which establishes minimum rules on the definition of offences and sanctions related to money laundering. At present, there are differences in the definition of money laundering offences and sanctions applied across the EU. These differences negatively affect cross-border police and judicial cooperation and may lead to "forum shopping" by offenders choosing to commit their crimes in the jurisdictions providing for lower sanctions. Non-cash payment fraud and cybercrime are included in the list of "predicate offences" (the underlying criminal activities generating the proceeds which are then laundered).

3. regulate the payment process, in particular to **facilitate secure payments** across the EU. These include:
   - Revised Payment Services Directive (PSD2)[19], which defines a comprehensive framework for the provision of payment services in the European Economic Area by, among others:
     - setting higher security standards for payments and better protecting consumers against current threats;
     - defining key terms such as "payment instrument";
     - specifying the conditions for the liability of the services provider and the payer;
     - providing for mandatory reporting to the competent authority of major operational or security incident relating to the account information service provider or the payment initiation service provider.
     - requiring Member States to ensure that payment service providers provide, at law enforcement on an annual basis, statistical data on fraud relating to different means of payment.
   - Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing,[20] (the fourth Anti-Money Laundering Directive), which aims at better identifying suspicious transfers (including those resulting from non-cash payment fraud) and communicating them through suspicious transaction reports to national Financial Intelligence Units (FIUs).

     The extension of the scope of the fourth Anti-Money Laundering Directive to virtual currencies exchange platforms and custodian wallet providers is currently under discussion. It aims to ensure a clearer regulatory framework

[18] Proposal for a Directive of the European Parliament and of the Council on countering money laundering by criminal law COM/2016/0826 final - 2016/0414 (COD)
[19] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
[20] Directive 2015/849/EU of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

and more transparency (due diligence) for exchanges between virtual and fiat currency.

- Regulation (EU) 2015/847 on information accompanying transfers of funds[21], which sets out rules on the information on payers and payees, accompanying transfers of funds, in order to help prevent, detect and investigate money laundering and terrorist financing.
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market[22] (Electronic Identification and Trust Services (eIDAS) Regulation), which aims to improve trust in EU-wide electronic transactions and to increase the effectiveness of public and private online services and e-commerce by, e.g. removing existing barriers to the use of eID in the EU.
- Regulation (EU) 2012/260 establishing technical and business requirements for credit transfers and direct debits in euro[23], which created the Single Euro Payments Area (SEPA) and supported the integration of the euro payments market by developing harmonised payment schemes, frameworks for electronic euro payments and mobile and online payments.
- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[24], which aims at enhancing the overall level of cybersecurity in the EU. It provides Member States with a coordination mechanism to support a swift and good operational cooperation on specific cybersecurity incidents and the sharing of information about risks.

In addition to the above legislative acts, the legislation resulting from the data protection reform[25] is of critical importance in the context of combatting non-cash payment fraud:

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[26] (General Data Protection Regulation).
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

[21] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)
[22] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[23] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009
[24] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[25] See here for more information
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data[27].

Last but not least, the fight against non-cash payment fraud needs to be seen in the context of three important EU policies:

- the European Agenda on Security[28], which sets out the principles for EU action to respond effectively to security threats and the main steps planned by the European Commission to implement these, and identifies the 3 priorities for immediate action, by both national governments and the EU institutions, which share responsibility for EU security: 1) preventing terrorism and countering radicalisation; 2) fighting organised crime; 3) fighting cybercrime.
- the EU Cybersecurity Strategy[29], which aimed at creating the world's most secure online environment in the EU, by providing for partnerships with the private sector and non-governmental organisations or interest groups, and concrete action to protect and promote citizens' rights. The current 2013 version is being revised and an updated strategy is expected by the end of 2017.
- The Digital Single Market Strategy[30], which sets out 16 targeted actions based on 3 pillars: 1) Better access for consumers to digital goods and services across Europe, 2) Creating the right conditions and a level playing field for digital networks and innovative services to flourish and 3) Maximising the growth potential of the digital economy.

The Framework Decision today[31]

The Framework Decision contributes to the above EU policy context by covering with criminal law a specific set of offences related to the payment process, i.e. those involving fraud and counterfeiting of non-cash means of payment.

[27] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[28] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, COM(2015) 185 final

[29] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An open, Safe and Secure Cyberspace (JOIN(2013) 1 final of 7.2.2013)

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe - COM(2015) 192 final

[31] The relations and complementarity of the Framework Decision with other EU policies is further analysed throughout the document, in particular in sections 1.3 (problem drivers), 1.7 and annex 5 (evaluation of the existing policy framework). The coherence with EU policies of a possible initiative replacing the Framework Decision is analysed in particular in sections 3.3. (consistency with other EU policies and objectives) and annex 4 (coherence criteria)

That said, the European Agenda on Security acknowledges that the Framework Decision no longer reflects today's realities and insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.

While a full evaluation according to the Commission's Evaluation Guidelines was still to be conducted, by the publication of the European Agenda of Security in 2015 other exercises had provided information about the state of implementation and the strengths and weaknesses of the current legal framework. Two implementation reports were completed in 2004[32] and 2006[33]. In addition, relevant national provisions on non-cash payment fraud had recently been analysed under a Commission study on criminal sanction legislation and practice in representative Member States.[34] Furthermore, operational action under the EU policy cycle to tackle organized and serious international crime[35] had provided additional evidence as to the effectiveness of the existing rules.

Consequently, the Commission committed in the European Agenda of Security to review the existing legislation on combatting fraud and counterfeiting of non-cash means of payments.

President Juncker reiterated that commitment by including improved rules on fraud in non-cash payments in his September 2015 Letter of Intent, initially planned for delivery in 2016:

> *"**Priority 7: An Area of Justice and Fundamental Rights Based on Mutual Trust***
>
> – *Follow up to the European Agenda on Security, including a proposal reviewing the framework decision on terrorism, improved rules on firearms **and fraud of non-cash payments**, and corresponding operational measures"*[36]

Stakeholders and citizens had the opportunity to express their views in an open public consultation through an online questionnaire that was accessible from 1/3 to 24/5/2017. The Commission organized as well targeted consultations with stakeholders from the public and private sector and civil society organisations. An external contractor also organized targeted consultations through interviews and an online survey, within a study on the evaluation of the current policy and legislative framework and impact assessment.

In general, stakeholders expressed doubts about the relevance, effectiveness and added value of the Framework Decision, and indicated the need to improve cooperation between national authorities and between public authorities and the private sector.

---

[32] Report from the Commission based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM/2004/0346 final

[33] Report from the Commission - Second report based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM/2006/0065 final

[34] Study on criminal sanction legislation and practice in representative Member States, p178-232

[35] The policy cycle is a methodology adopted in 2010 by the European Union to address the most important criminal threats affecting the EU. Each cycle lasts four years and optimises coordination and cooperation on chosen crime priorities. More information is available here and here.

[36] Letter from Commission President Juncker and First Vice-President Timmermans to the Presidents of the Parliament and the Council of the EU, 9 September 2015

www.parlament.gv.at

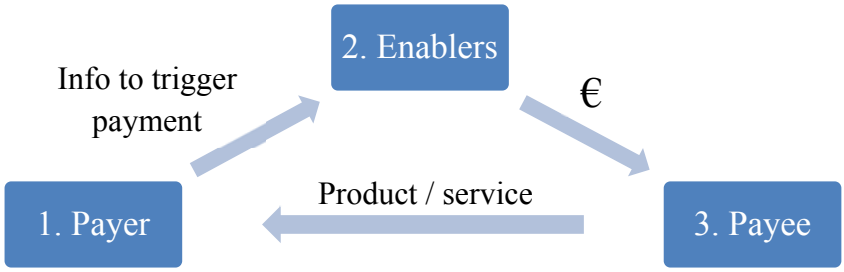
1.2. Definition and magnitude of the problem

1.2.1. Payments

There are 3 main parties in any payment: the one who pays (payer), the one who gets paid (payee) and the one who executes the payment (enabler).

The payer shares with the enabler the necessary information to authorize it to give the funds to the payee, who in return provides products or services to the payer.

Figure 1: main parties and exchanges in a payment



Source: European Commission

For example, when someone (payer) buys a book in an online shop (payee), he shares with his bank and credit card company (enablers) the necessary information to trigger the execution of the payment and give the online shop the money in exchange for the book.

As the example above illustrates, there are three types of enablers:

1. Financial institutions (e.g. a bank): provide the monetary value.
2. Payment instruments (e.g. a credit card): provide the vehicle to convey the monetary value.
3. Providers of other services related to the execution of the payment (e.g. enablers of a credit card transaction).

In cash payments, a central bank provides the monetary value, which is conveyed in bills and coins (payment instruments). In non-cash payments there is a wider variety of payment instruments.

1.2.2. Non-cash payments

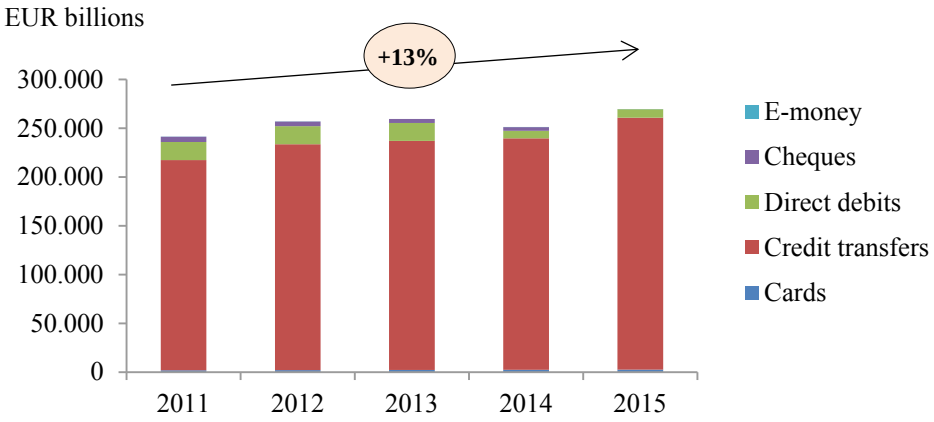
Taxonomy

The most common non-cash payment instruments are payment cards (credit and debit), credit transfers, direct debits, cheques, e-money, virtual currencies, mobile money, vouchers (e.g. tickets restaurant), coupons and fidelity cards.

Magnitude of the problem

The total **value** of non-cash payment transactions with **cards, credit transfers, direct debits, cheques and e-money** has been increasing in Europe in the last years:

Figure 2: value of transactions in key non-cash payment instruments in the EU[37]

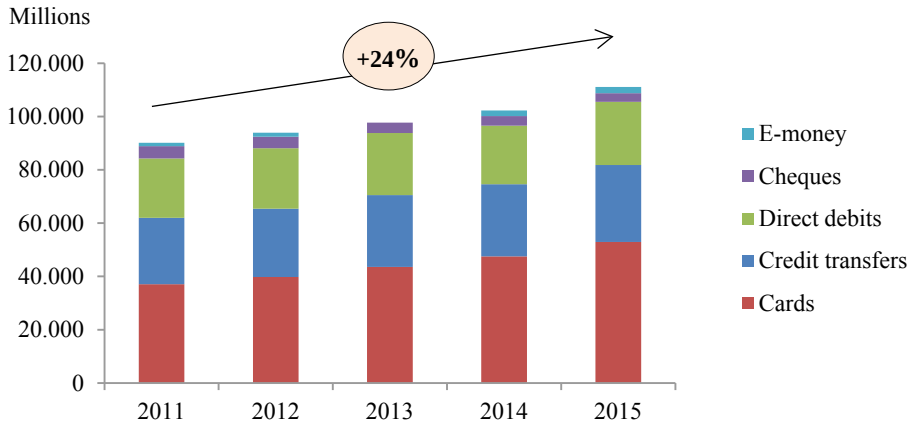


Source: European Central Bank, Payment Statistics, September 2016

The decrease in the **value** of transactions with cheques and direct debit has been compensated by the significant increase in the value of transactions with the other payment instruments, in particular credit transfers, which account for more than 90% of the total.

The total **number** of non-cash payment transactions with **cards, credit transfers, direct debits, cheques and e-money** has also been increasing in Europe in the last years:

Figure 3: number of transactions in key non-cash payment instruments in the EU[38]



Source: European Central Bank, Payment Statistics, September 2016

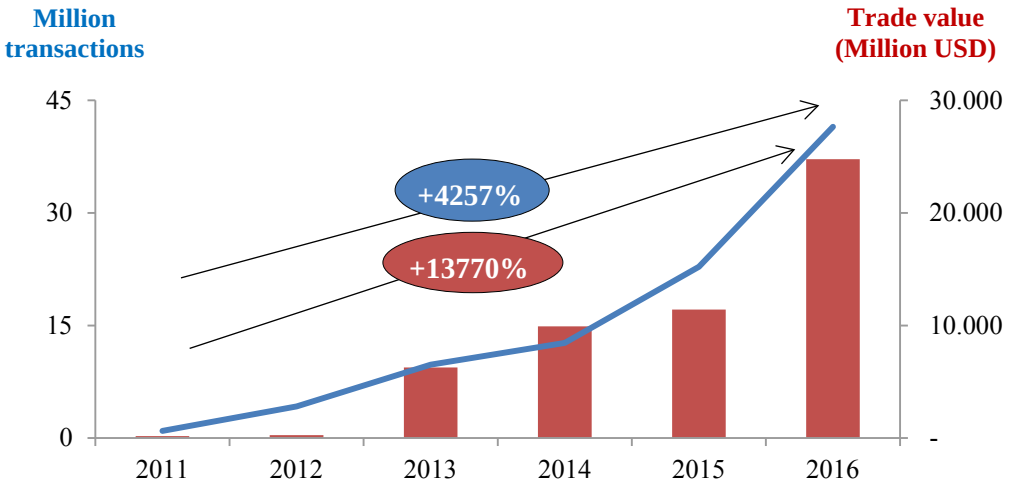
The decrease in the **number** of transactions with cheques has been more than compensated by the significant increase in the number of transactions with the other payment instruments.

Payments with **virtual currencies** have also dramatically increased in the last years globally, both in value and number:

[37] Indicated growth of 13% corresponds to a 3% compounded annual growth rate (CAGR), over the 2011-2013 period

[38] Indicated growth of 24% corresponds to a 5% CAGR over the 2011-2013 period

Figure 4: value and number of transactions with bitcoin globally[39]



Source: blockchain.info/stats, accessed on June 2017

Although the data on **mobile payments** is limited, a 2016 study indicated that 54% of European consumers regularly use their mobile device to make payments, three times as many as in 2015.[40]

For vouchers, coupons and fidelity cards no data about market size and number of transactions could be located, although these payment instruments are likely to represent a very small fraction of the total number of transactions and value of non-cash payments.

1.2.3. Fraud in non-cash payments

Taxonomy

Fraud can affect each of the 3 main parties/stages in a payment described in figure 1.

In non-cash payments, fraud takes the following forms in each of the stages:

1) Trigger the execution of payments by using payer information fraudulently.
   The fraudster gets hold of the information required to trigger the execution of a payment and uses it for his own benefit, against the will of the legitimate owner of the funds.
   There are multiple methods to collect that information: phishing, skimming, pharming[41]… or simply acquiring it from someone else.
   Once the fraudster has acquired the necessary information, he can use payment instruments (in particular non-corporeal such as card credentials, credit transfers, direct debit and virtual currencies) to trigger the execution of a payment.

[39] CAGR (2011-2016): number of transactions = 113%, value of transactions = 168%
[40] Digital Payments study, Visa, 2016
[41] See glossary. Additional information is available at http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/

2) Execute payments by tampering with or stealing the payment instrument.
    - Tampering with payment instruments:
        - Counterfeiting: e.g. of cards (credit/debit, fuel, loyalty) out of stolen card credentials to pay in stores or withdraw cash in ATMs; counterfeiting of cheques, vouchers or coupons, etc.
        - Hacking of information systems to process payments: e.g. tampering with points of sale for card transactions; unlawfully increase the credit card limit to allow excess expenses go undetected, etc.
    - Stealing payment instruments.
3) Fail to provide the product/service after receiving the payment.
   This type of payment fraud covers the various forms of scams, from failing to deliver the product/service as initially agreed, to tricking the payer to trigger the payment (e.g. CEO fraud, in which the attacker pretends to be the CEO of a company and tricks an employee at the organisation into wiring funds to the fraudster). This third category is out of the scope of this impact assessment.

Magnitude of the problem

Fraud data exists only for card fraud which, as shown in figure 3, is the most important non-cash payment instrument in terms of number of transactions.[42]

There are two kinds of card fraud:

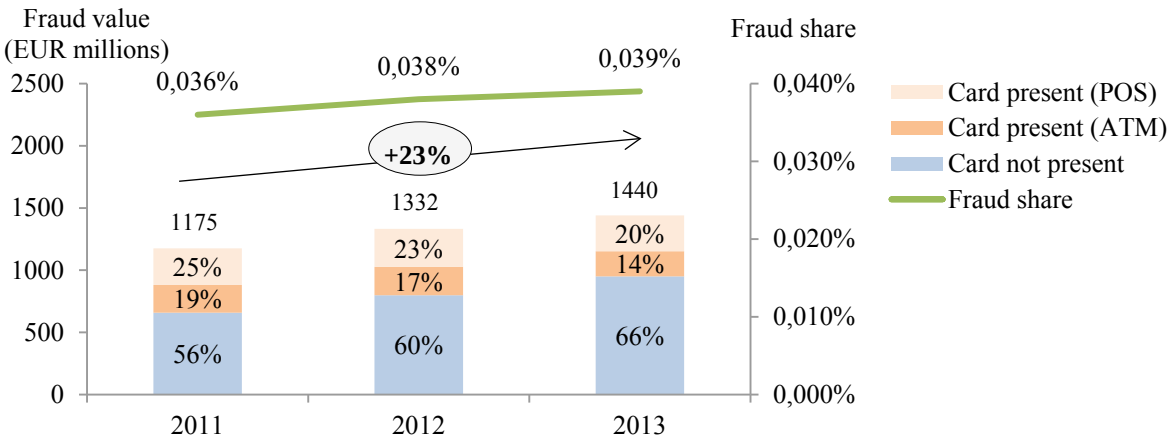
- The card is present, e.g. using a counterfeit card to withdraw cash from an ATM or to pay in a point of sale in a shop.
- The card is not present, e.g. when using stolen card credentials to buy goods online.

The total **value** of card fraud using cards issued in the Single European Payment Area (SEPA) amounted to **€1.44 billion** in 2013 (most recent data available[43]), of which 66% (€950 million) corresponded to card-not-present fraud and 34% (€490 million) to card-present fraud (of which 20% to point-of-sale (POS) and 14% to ATM fraud). This represented 0.039% of the total value of card transactions:

[42] It was not possible to find fraud data of other means of non-cash payment at EU level. By considering only card fraud, the size of the problem is being underestimated. That said, national data from the UK (Financial Fraud Action UK, Fraud The Facts 2016, p11) indicates that card fraud represented 75% of the total financial losses in 2015, followed by remote banking (22%) and cheques (3%). Assuming that similar proportions occur at EU level, the actual volume of fraud would at least be 25% higher than card fraud. These estimates also exclude fraud with virtual currencies and mobile payments, for which no data could be located.

[43] This data was calculated combining transaction data received from 23 card payment schemes, including Visa Europe, MasterCard Europe and American Express. A comparison of this transaction data with data held in the ECB's Statistical Data Warehouse suggests that the data available for 2013 represent 100% of the total value of transactions within the EU. However, this figure must be treated with caution, as it may reflect both gaps in the Statistical Dara Warehouse and double counting in data reported for oversight purposes (see European Central Bank, Fourth Report on Card Fraud, 2015, p5)

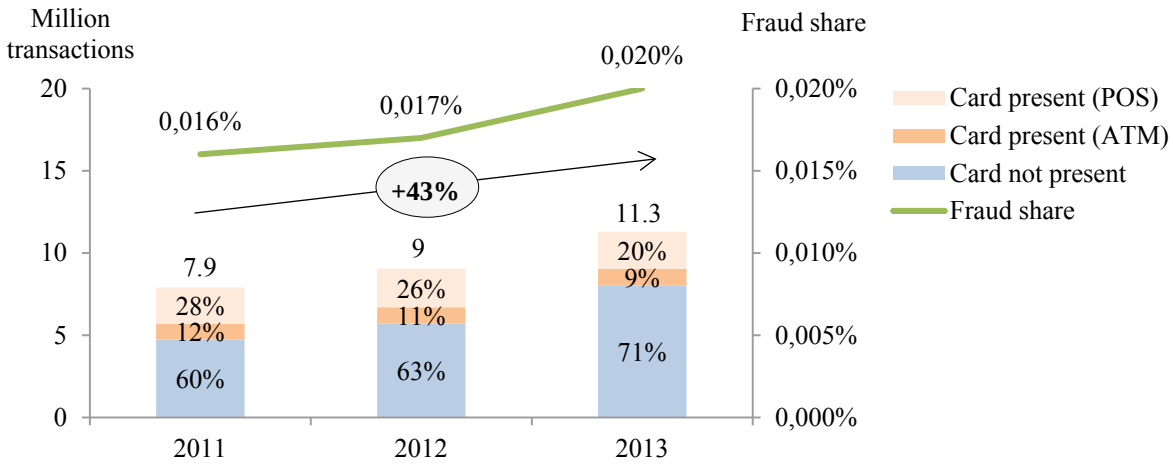
Figure 5: evolution of the total value of card fraud using cards issued within SEPA[44]



Source: European Central Bank, Fourth Report on Card Fraud, 2015

The total **number** of fraudulent transactions using cards issued in SEPA amounted to **11.29 million in 2013**, of which 71% corresponded to card-not-present fraud and 29% to card-present fraud (of which 20% to POS and 9% to ATM fraud). This represented 0.020% of the total number of card transactions:

Figure 6: evolution of the total volume of card fraud using cards issued within SEPA[45]



Source: European Central Bank, Fourth Report on Card Fraud, 2015

As figures 5 and 6 indicate, **card-not-present** fraud not only constitutes the largest share of card fraud but also a share that has increased in the last years, both in value and in number of transactions. Moreover, the increase in the total amounts of card fraud in the last years (both in value and in number of transactions) has been mainly driven by the increase in card-not-present fraud.

[44] Indicated growth of 23% corresponds to a 3% CAGR over the 2011-2013 period
[45] Indicated growth of 43% corresponds to a 20% CAGR over the 2011-2013 period

Card-present fraud (i.e. ATMs and POS terminals) decreased in 2013, due to:[46]

- Near completion of migration to the EMV standard (cards with chip) within SEPA.
- Wider use of blocking overseas transactions using EU-issued cards unless they have been activated in advance.
- Increased physical security measures at the terminal (e.g. lids to protect PIN entry, skimming device detectors, etc…).
- Deactivation of the option to fall back to magnetic stripe usage for cards.

Card-present fraud is roughly equally divided in value into counterfeiting (45%) and fraud using lost or stolen cards 43% (2013).[47]

1.2.4. Why is it a problem

Box 1 puts into perspective the magnitude of the problem described above:

Box 1: the magnitude of the problem put into perspective

- Average loss per fraudulent card transaction: around **EUR 130** (result of dividing the value of card fraud, EUR 1440 million, by the number of card transactions, 11.3 million, in 2013).

- The average monthly salary in the EU is around EUR 1500 (EUR 1489 in 2014[48]). Losing around 10% of the monthly salary due to fraud (a conservative estimate since there is only card fraud data available) is a significant amount which becomes much more relevant for the citizens earning below the average EU salary (for example, these fraud losses would have represented **more than two thirds** of the minimum wage in Bulgaria of EUR 173 in 2014[49]).

- The probability of a card transaction being fraudulent was 0.002% in 2013, as indicated in figure 6, or **1 in 5000**. This was about 4 times more likely than dying on a road traffic accident in the same year, all vehicles combined, and including pedestrians.[50]

The most problematic aspect of non-cash payment fraud is that it represents **a threat to security.** In addition, it is **an obstacle to the digital single market.**

[46] European Central Bank, Fourth Report on Card Fraud, 2015
[47] ibid.
[48] Reinis Fischer, Average Salary in European Union, 2014
[49] Reinis Fischer, Minimum Wages in European Union, 2014
[50] Eurostat, Road accident fatalities - statistics by type of vehicle, 2014

A threat to security

Non-cash payment fraud provides income for organized crime and therefore enables other criminal activities such as terrorism, drug trafficking and trafficking in human beings. In particular, according to Europol, non-cash payment fraud income is used to finance:

- Travel:
  - Flights: the experience gained from conducting the Global Airline Action Day[51] operations from 2014 to 2016 indicates a clear link between non-cash payment fraud, airline ticketing fraud and other serious and organised crimes, including terrorism. Some of the people travelling on fraudulently obtained tickets were known or suspected to be involved in other offences.
  - Other travel fraud (i.e. selling and travelling on tickets that have been obtained fraudulently). The main way to purchase illegal tickets was through the use of compromised credit cards. Other methods included, e.g. the use of compromised loyalty point accounts, phishing travel agencies and voucher fraud. In addition to offenders, those travelling on fraudulently obtained tickets included victims of trafficking and people acting as 'money mules'.
- Accommodation: law enforcement also reports that non-cash payment fraud is also used to facilitate other crimes that require temporary accommodation such as trafficking in human beings, illegal immigration or drug trafficking.

Europol also reported that the criminal market for payment card fraud in the EU is dominated by well-structured and globally active organised crime groups.[52]

Whereas 0.0039% of the value of all card transactions being lost to fraud may seem a small percentage, this represents a total amount of at least **EUR 1,44 billion per year going to fund organized crime groups**. This amount is likely to increase, as described later in section 1.6 ("How would the problem evolve"), mainly fuelled by the increasing digitalisation of the economy and the emergence of new payment instruments (technological innovation).

An obstacle to the digital single market

Non-cash payment fraud hinders the development of the digital single market in two ways:

- It causes important direct economic losses. Section 1.2.3 quantified non-cash payment fraud in Europe in terms of the amount of direct fraud losses for which

[51] More details here
[52] Situation Report: Payment Card Fraud in the European Union, Europol, 2012

there is data available (card fraud). For example, the airlines lose around USD 1 billion per year globally in card fraud.[53]

- It reduces consumers' trust, which may result in reduced economic activity and limited engagement in the digital single market. According to the most recent Eurobarometer on Cyber Security,[54] the vast majority of Internet users (85%) feel that the risk of becoming a victim of cybercrime is increasing. Whereas the probability of 0.002% (1 in 5000) of a card transaction being fraudulent may seem small, the **perception** of insecurity has 42% of users are worried about the security of online payments. Because of security concerns, 12% are less likely to engage in digital transactions such as online banking.

1.3. Problem drivers

To analyse in detail the problem of non-cash payment fraud and identify its drivers, the Commission conducted an evaluation of the Framework Decision (see annex 5). The evaluation also analysed other EU legislative instruments put in place since the adoption of the Framework Decision, which are relevant to tackling non-cash payment fraud, and incorporated the input from the public consultation and expert meetings organized by the European Commission.

The evaluation detected three problem drivers:

1. Some crimes cannot be **effectively investigated and prosecuted** under the current legal framework.
2. Some crimes cannot be **effectively investigated and prosecuted** due to **operational obstacles**.
3. Criminals take advantage of gaps in **prevention** to commit fraud.

The problem drivers indicate that the issue at hand is mostly a **regulatory failure,** where the current EU legislative framework (the Framework Decision) has become partially obsolete, due mainly **to technological developments.** The evaluation indicated that this regulatory gap has not been sufficiently covered by more recent legislation, as the analysis of the problem drivers below will also highlight.

The drivers are divided into the following sub-drivers:

[53] IATA, 2015
[54] Special Eurobarometer 423, Cyber Security, February 2015

www.parlament.gv.at

Table 1: drivers and sub-drivers

Drivers	Sub-drivers
1. Some crimes cannot be **effectively investigated and prosecuted** under the current **legal framework.**	a. Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised. b. **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised. c. Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States. d. Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution**.**
2. Some crimes cannot be **effectively investigated and prosecuted** due to **operational obstacles.**	a. It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution. b. Under-reporting to law enforcement due to constraints in **public-private cooperation** hampers effective investigations and prosecutions.
3. Criminals take advantage of gaps in **prevention** to commit fraud.	a. **Information sharing** gaps in **public-private cooperation** hamper prevention. b. Criminals exploit the **lack of awareness** of victims.

1.3.1. Some crimes cannot be effectively investigated and prosecuted under the current legal framework

a. Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised.

The Framework Decision contains a definition of payment instrument (Art. 1(a)) that technological developments have rendered obsolete.

The definition does not explicitly include **non-corporeal** payment instruments such as virtual currencies, e-money and mobile money, which are growing in importance as previously described and as stakeholders highlighted in the consultation.
It could be understood that non-corporeal instruments are implicitly included in Art. 3 on offences related to computers, which requires Member States to sanction fraudulent forms of conduct relating to the use of computer data and computer programmes or systems. However, the Framework Decision does not include any definition of "**computer data**" or "**computer programme/system**", and therefore it is not possible to clearly identify the types of payment instruments that are covered. For example, does "computer" include mobile devices? Does computer data relate only to data stored in computers or is data stored in 'the cloud' also covered? The lack of a definition of "computer data" or "computer programme/system" creates a grey area in a criminal law instrument, not properly covering behaviours that are gaining more and more importance through the increasing dematerialisation of payment instruments and the opportunities that Internet offers for payment transactions.

Also, without a **technology neutral** definition, not only the payment instruments currently explicitly mentioned risk becoming obsolete (e.g. as eurocheques and eurocheque cards have already become) but also, if new payment instruments emerge in the future, it is unclear whether the Framework Decision would be able to cover them.

The Payment Services Directive (PSD2)[55] contains a broader definition of payment instrument:[56]

> "*Payment instrument shall mean any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order*."

[55] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
[56] Article 14(14)

The formulation "set of procedures" covers non-corporeal payment instruments and in particular e-money. This definition includes most of the main non-cash means of payment, i.e. those covered by the Framework Decision plus e-money, mobile money, virtual cards, electronic ticket restaurants, virtual coupons and electronic wire transfers and direct debits.

Since the Payment Services Directive is not a criminal law instrument, the fact that the definition in it covers a number of non-corporeal payment instruments does not imply that offences involving these instruments are criminalised.

In addition, this definition is not entirely **technology neutral** as it does not cover those that do not initiate a payment order (e.g. fidelity/loyalty cards) and those that are not personalised (e.g. virtual currencies or some types of coupons).

The Attacks Against Information Systems Directive (AAIS)[57] is a criminal law directive which contains definitions of information system (a broader term than "computer") and computer data:[58]

> *"(a) 'information system' means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;*
>
> *(b) 'computer data' means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function;"*

These definitions are general enough to encompass **non-corporeal** payment instruments.

That said, this Directive focuses on criminalizing attacks against information systems, which is not necessarily the same as non-cash payment fraud, as we will see in more detail in the offences section below. For example, it criminalises the illegal access to information systems but only when a security measure has been infringed. A fraudster using legitimate (but stolen) credit card credentials to shop online would not necessarily infringe any security measures.

The expert meetings and the consultation confirmed a gap in the current definitions as some payment instruments are not covered, considering it one of the most important obstacles to investigation and prosecution. In general, the **lack of a technology neutral**

[57] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
[58] Articles 2(a) and (b) respectively

legal framework is a key factor behind the current **regulatory failure** that a potential initiative would need to address.

b. **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised.

Using the taxonomy of non-cash payment fraud in section 1.2.3, based on figure 1, the stage of triggering the execution of payments by using payer information fraudulently includes two sets of behaviours: (i) **preparatory acts**, i.e. the collection (e.g. phishing, skimming), trade (e.g. carding websites), making available (e.g. dumping) and possession of payer information; (ii) the actual **use** of the payer information.

The Framework Decision covers the **use** of the payer information to trigger the execution of the payment in Art. 3 ("… without right introducing, altering, deleting or suppressing computer data, in particular identification data"). However, the use of unlawfully appropriated computer data covered by Art. 3, is criminalised only when offences intentionally result in a **transfer of monetary value**. This means that **preparatory acts** that precede fraud without being directly linked to it are excluded from Art. 3.
Moreover, Art. 4 covers the "fraudulent making, receiving, obtaining, sale or transfer to another person or the possession of computer programmes the purpose of which is the commission of any of the offences described under Art. 3." This article also raises the issue of a lack of definition of a computer (programme). In addition, the use of these computer programmes is not explicitly mentioned and in some cases it may not be necessary to possess them to be able to use them (e.g. they might be used from the cloud).

Art. 5 covers "attempt" but since it does not contain a definition of "attempt", it is not possible to determine whether preparatory acts would be included.

Experts from the Member States confirmed the need for a criminalisation at EU level of preparatory acts (in particular phishing), during the expert meetings.

The Attacks Against Information Systems Directive criminalises the "intentional production, sale, procurement for use, import, distribution or otherwise making available… of… a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed."[59], with the intention to gain illegal access to information systems by infringing a security measure.[60] As discussed earlier, a fraudster using legitimate (but stolen) credit card credentials to shop online would not necessarily infringe any security measures.

c. Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States.

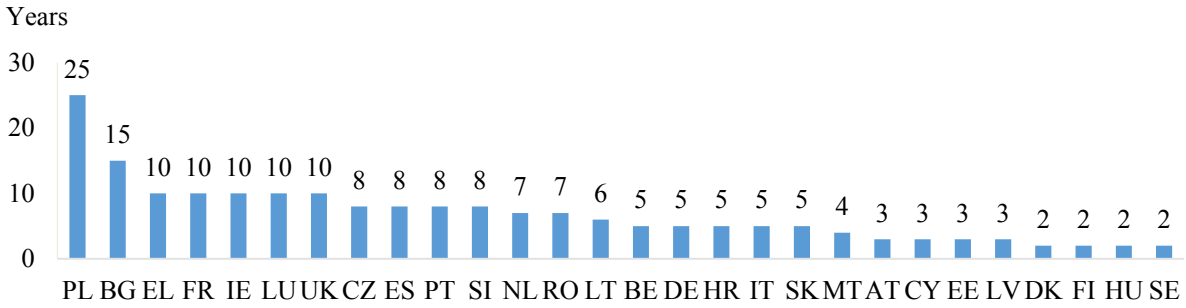
[59] Article 7(b)
[60] Article 3

www.parlament.gv.at

The Framework Decision requires Member States to set up criminal penalties that are effective, proportionate and dissuasive, without specifying minimum levels. As a consequence, Member States have adopted different levels of penalties.

Whereas all Member States include, at least for serious cases, penalties of imprisonment, these vary significantly. For example, figure 7 shows the variation in the level of maximum number of years of imprisonment for counterfeiting or falsification of payment instruments (Art. 2(b)):

Figure 7: maximum penalties across Member States for Art. 2(b) offences



Source: EY

The Attacks Against Information Systems Directive determines maximum level of penalties of at least 2 years for the offences it contemplates (illegal access to information systems, illegal system interference, illegal data interference, illegal interception, offences related to tools for committing offences and inciting, aiding, abetting and attempt). It also determines maximum level of penalties for aggravating circumstances from at least 3 years to at least 5 years, depending on the situation.

Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (fourth Anti-Money Laundering Directive) defines a range of administrative sanctions and measures which can be imposed to obliged entities that do not comply with the preventative framework put in place by this Directive.

There were different views expressed at the expert meetings concerning the need to have a certain level of penalties specified in EU legislation. Some experts saw value in having similar level of offences across the EU, to facilitate cross-border cooperation and ensure a minimum level of deterrence. Other experts questioned the deterrence effect of penalties versus other factors such as the likelihood of being arrested. They also questioned the "forum-shopping" effect, where criminals would tend to operate in countries with lower levels of penalties, by arguing that, if it were true, it would be happening already, but there is no evidence of that. They expressed preference for determining the sanctions based on the gravity of the crime, rather than to facilitate investigations (some investigative tools are only available to crimes that have a certain level of penalties, see

www.parlament.gv.at

the section on cross-border cooperation below). That said, there was a certain consensus of having a level of penalties set at EU level coherent with other EU instruments (e.g. Attacks Against Information Systems Directive, European Arrest Warrant…), as long as it was limited to serious offences.

d. Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution**.**
The Framework Decision specified a limited set of situations in which a Member State could claim jurisdiction: when the offence was either committed in its territory, or abroad by one of its nationals (on condition of double criminality, i.e. provided that it was also an offence abroad) or for the benefit of a legal person stablished in its territory. The last two situations could be optional based on whether the Member State extradited its nationals, a possibility that the European Arrest Warrant has rendered partially obsolete (see extradition section below).

The biggest challenge concerning jurisdiction in non-cash payments is the cross-border nature of the crime combined with the access to digital evidence, as non-cash payment fraud increasingly has a digital component.

To give an idea of the complexity of the issue, please consider the case of Hans, a **German** national working and living in **Poland**, where he has his bank account. Unfortunately, while on vacation in **Romania**, his credit card details were stolen via skimming when he paid a taxi that was cooperating with an organized crime group. This group sold his credit card details to a carding website hosted in the **Netherlands**, where a **Portuguese** national bought his card details for just €20. He later used them from his apartment in **Italy** (or at least from an IP address that pointed to Italy but he might very well have used a VPN to connect from his summer house in the Portuguese Algarve), to buy goods online in a website hosted in **France** (but belonging to a multinational company based in **Ireland**) to be shipped from **Spain** to his cousin in **Luxembourg**.

While this is a fictional case, representatives from law enforcement, the judiciary and the private sector described in the expert meetings similar situations, involving as many jurisdictions, to illustrate the challenges they face while investigating non-cash payment fraud. The main risk is that crimes might not be investigated because no country claims jurisdiction or that the lack of judicial cooperation makes the cross-border investigation process impossible in practice.

The Framework Decision provides limited tools to address these challenges. For example, coming back to Hans, when he sees the illegal activity in his credit card and informs the Polish authorities, they would not be able to claim jurisdiction on the basis of the Framework Decision only (offence neither committed in its territory nor by one of its nationals not for the benefit of a legal person established in Poland).

Overall, a majority of Member States (22)[61] have extended their jurisdiction beyond the requirements of the Framework Decision in a variety of ways. As pointed out in the expert meetings, these differences in the implementation increase the complexity of the attribution of jurisdiction of cross-border offences, which may result in longer prosecution times and, in some cases, no prosecution at all.

The Attacks Against Information Systems Directive includes broader jurisdiction rules than the Framework Decision, by, for example, eliminating the condition of double criminality and including situations in which the offender is physically present in the Member State, regardless of whether the information system attacked is in the same Member State, and vice versa, when the information system is in the Member State, regardless of where the offender is located.

The Commission committed in 2016 to addressing the challenges for investigations in cyber-enabled crimes in its Communication on Delivering on the European Agenda on Security[62], aiming to propose solutions by the summer of 2017.

In its Conclusions on improving criminal justice in cyberspace[63], adopted on 9 June 2016, the Council supported the Commission´s commitment and called on the Commission to take concrete actions based on a common EU approach to improve cooperation with service providers, make mutual legal assistance more efficient and to propose solutions to the problems of determining and enforcing jurisdiction in cyberspace.

The Commission conducted an expert consultation process and summarized its results in a non-paper[64], presented to the Council on June 8 2017, which may result in a legislative initiative.

1.3.2. Some crimes cannot be effectively investigated and prosecuted due to operational obstacles

a. It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution.

Stakeholders pointed out during the evaluation and consultation the fact that **it takes a long time to receive the information requested from another Member State,** when that information is received at all:

1) First, it takes time to **set up the procedure** to exchange the information between the Member States, in particular when this requires the authorisation of multiple authorities.

[61] AT, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, LT, LV, MT, PL, PT, RO, SE, SI, SK, UK
[62] COM(2016) 230 final
[63] Council conclusions on improving criminal justice in cyberspace
[64] Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward

2) Second, it takes time for the Member State asking to **understand** what can be requested, and for the Member State asked what is being requested (including the urgency of the request), given the significant differences that still exist in their legislative frameworks, such as those concerning:
    - **Prescription periods**, both in terms of duration and of the moment the period starts to count (e.g. when the offence is completed or when the victim discovers the fraud). The duration is usually linked to the severity of the maximum penalties, which, as discussed, vary significantly across Member States.
    - **Data retention** rules, following the 2014 sentence of the Court of Justice of the European Union[65] declaring invalid the Data Retention Directive[66], as well as **data protection** rules (to be harmonized with the new General Data Protection Regulation[67], which enters into force in May 2018, and the directive regulating the processing of personal data by authorities[68], which Member States have until May 2018 to transpose).
    - **Confiscation rules**: while some Member States follow a "follow-the-money" approach and prioritise the asset recovery, other focus on tracking and retaining the perpetrator.
3) Last but not least, it takes time to **produce** the information requested:
    - The information may not be **ready available**. When the information needs to be collected in the Member State, there can be **coordination issues** at the national level between law enforcement and judicial authorities for the exchange of information.

      If an **investigation** needs to be open to collect the information, a new set of issues appears, such as:
        - Lack of adequate **investigative tools**, in particular to investigate fraud with a cybercrime component (e.g. IT forensics, decryption, attribution).
        - Lack of **skills** in law enforcement and the judiciary to deal with non-cash payment fraud cases of certain technological sophistication.

[65] See the press release at https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
[66] Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
[67] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
The EU data protection legislation shall also be seen relevant in this respect as the credit card number shall be considered as personal data. Moreover, credit card also contains other personal data such as the name of a citizen. The current Directive 95/46/EC imposes obligations on data controllers (such as banks) on security of processing of personal data. The upcoming General Data Protection Regulation 2016/679 modernises the rules on security of personal data. In addition, the new legislation imposes an obligation of a notification of personal data breaches such as unlawful processing of personal data to the national data protection supervisory authorities and to the data subject in certain circumstances. Non-compliance with such rules will be subject to administrative fines.
[68] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

- Limited **capacity** of law enforcement, which causes other criminal offences to be prioritized over non-cash payment fraud (compared to other criminal offences, non-cash payment fraud is underreported, frequently involves a high volume of small financial losses, and has a relatively low level of penalties).

Also, the lack of **public-private sector cooperation** can hinder the ability to collect information promptly.

- When the information involves **non-EU countries**, as is often the case in e.g. skimming and counterfeiting of credit cards, a new level of complication and delays is added.

Stakeholders emphasized multiple times the important role that **Europol** plays in helping overcome each of these obstacles, setting up communication channels, helping understand the requests and supporting Member States with its analytical capabilities and technical expertise.

The Framework Decision contains two articles focused on **cross-border cooperation**: Art. 11 (mutual assistance) and Art. 12 (exchange of information).
Art. 12 requires Member States to designate operational contact points for the exchange of information. It does not specify who those contact points should be or how the network should work (e.g. service hours or maximum time to respond to requests).

The Attacks Against Information Systems Directive also contains provisions on exchange of information through a network of contact points, with additional requirements on service hours and maximum time to answer urgent requests of assistance.

b. **Under-reporting** to law enforcement due to constraints in public-private cooperation hampers effective investigations and prosecutions.

The Framework Decision does not include any provisions on public-private cooperation.

Stakeholders that contributed to the consultation widely considered public-private cooperation an enabler to tackle non-cash payment fraud across all levers, from investigation and prosecution and assistance to victims to prevention, given that information concerning non-cash payment fraud is spread across multiple private sector actors.

The evaluation and stakeholder consultation found that the main **obstacles** that prevent public-private cooperation from reaching its full potential relate to **information sharing**, both domestically and cross-border:

- Lack of clarity on the requirements on private sector to collect information (e.g. data protection and data retention rules), which may affect the admissibility of evidence in court.
- Limited implementation by payment service providers of systems to monitor, handle and follow up on general security incidents (e.g. data breaches) and

www.parlament.gv.at

security-related customer compliance, and to notify the competent authorities (e.g. law enforcement). However, it shall be taken into account that the new data protection legislation contains rules on personal data breaches.

A specific case of information sharing is mandatory reporting to law enforcement, which contributes to gain a better understanding of the fraud case and therefore enables a better response and prevention:

- Reporting obligations for payment services providers exist in the Payment Services Directive (PSD2), in cases of major operational or security incidents, and in the fourth Anti Money Laundering Directive,[69] for "obliged entities" (which include financial institutions), in case suspicious transactions are detected.
- A majority of Member States (16)[70] make it mandatory to report to law enforcement whenever there are suspicions raised with regard to the commission of an offence relating to payment instruments, computers and/or specifically adapted devices.

Under-reporting is common in non-cash payment fraud, due to:

- Poor information available to victims on the reporting systems in place, and the role of actors involved in their protection, which often differ from one Member State to another.
- The long-tail nature of non-cash payment fraud, a crime that typically affects a relatively large number of victims but each crime involves the loss of a relatively low value, which may discourage reporting (this allows fraudsters to draw less attention from users and payment service providers, which in turn encourages future fraud).
- Reputational concerns of businesses, for example to expose publicly that they have been victim of data breaches.
- The compensation to companies and individuals received by banks, which may cause that the victims abandon the proceedings as soon as the reimbursement has been received.
- Victims of fraud may blame themselves and/or fear that others will blame them for stupidity or even culpability.
- Limitations in current reporting systems (e.g. lack of reporting mechanisms for internet crimes, lack of feedback to victims that report, lack of reporting categories).

1.3.3. Criminals take advantage of gaps in prevention to commit fraud

a. **Information sharing gaps** in **public-private cooperation** hamper prevention.

[69] Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

[70] AT, BG, CZ, DE, EE, EL, ES, FI, HR, IE, IT, LT, NL, PL, RO, SK

The information sharing gaps described above also affect public-private cooperation efforts on prevention.

For example, stakeholders pointed out that limited information sharing between the private sector and public authorities prevents the early identification of new threats, which is critical to ensure effective prevention.

b. Criminals exploit the **lack of awareness** of victims**.**
Representatives from victims' associations and other stakeholders pointed out that the lack of awareness of victims is a fundamental issue that drives non-cash payment fraud.

All types of stakeholders (payers, enablers and payees) could benefit from awareness raising campaigns to avoid falling victim of non-cash payment fraud. Cybercrime in general seems to be less known than the "regular" crimes and in some cases, taken less seriously, which increases the chances of becoming a victim of it.

To illustrate this, box 2 below describes how the lack of awareness of victims sustains the business model of phishing, a preparatory act for non-cash payment fraud:

Box 2: the economies of phishing[71]

According to a study by Cisco,[72] approximately **eight people out of a million** fall victim of phishing, with an average loss of $2,000 per victim.

Fully automated phishing kits to send phishing messages to 500,000 e-mail addresses can be bought online for just $65.
So, for only $130, criminals can generate $16,000, a 12,000% return on investment.
This explains why as many as 36 billion phishing messages are sent annually.

With more awareness from potential victims, the rate of people that would fall in the phishing trap would likely decrease.

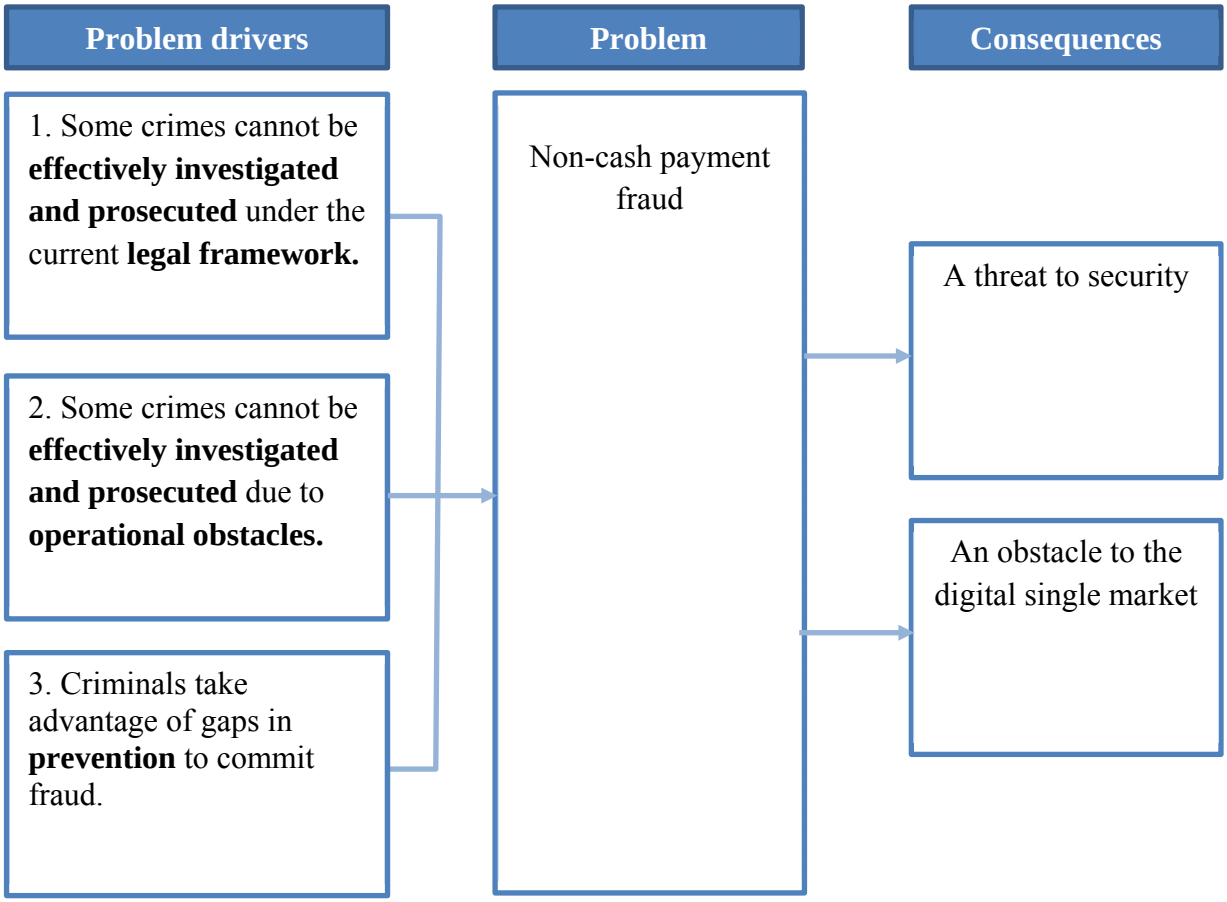
This driver focuses on prevention, which all types of stakeholders highlighted as an important area to be strengthened. Public-private cooperation can contribute to improving not only investigation and prosecution but also prevention. Therefore, the constraints to effective public-private cooperation appear in both drivers 2 and 3.

As specified in annex 5 (evaluation), most of the problems identified above (all except the long time needed to provide information in **cross-border cooperation** requests) can be attributed to shortcomings in the current EU legal framework rather than to a lack of implementation of existing EU rules.

[71] Future Crimes: Inside the Digital Underground and the Battle for Our Connected World, Marc Goodman, 2015
[72] Email Attacks: This Time is Personal, Cisco, 2011

The following **problem tree** summarizes the links between the drivers and the consequences of concern for the problem of non-cash payment fraud:

Figure 8: problem tree for non-cash payment fraud



1.4. Who is affected and how

To guide the mapping of the stakeholders affected by non-cash payment fraud we can use the overview of the basic parties involved in a payment described in section 1.2.1. and shown in figure 1: those who pay (payers), those who get paid (payees) and those who execute the payments (enablers).

Payers

The payer shares with the enabler the necessary information to authorize it to give the funds to the payee, who in return provides products or services to the payer.

This information is therefore very valuable for criminals. When the payer is a natural person, this information contains personal data (e.g. name, date of birth, identity card number), as well as other information necessary to trigger the payment (e.g. PIN and other bank and security details for operating online services such as login name and password).

Criminals steal this information in a variety of ways (e.g. skimming, shimming, phishing, data breaches).

Payers are affected in two ways when criminals use this information to:

1) trigger fraudulent payments that entrain a financial loss for the payer, or
2) impersonate the victim and cause damage in multiple other forms, ranging from psychological and social distress to the various consequences of reputational damage (e.g. tangible ones like negative impact in credit rating history, criminal record or inclusion in defaulter lists, and intangible ones like damaged relationships).

Enablers

There are basically three types of enablers:

1. Financial institutions (e.g. a bank), which provide the monetary value.
2. Payment instruments (e.g. a credit card), which provide the vehicle to convey the monetary value.
3. Providers of other services related to the execution of the payment (e.g. enablers of a credit card transaction).

The enablers are referred to as "payment service providers" in the Payment Services Directive (PSD2).

Enablers suffer the consequences of fraud in two ways: through the loss of business opportunities due to lack of trust of the payers and through the direct losses caused by the fraud:

1) As described in the previous section, non-cash payment fraud reduces the trust of consumers, which may result in the unwillingness to use some payment services, in particular the digital ones. This results in lost business opportunities for the enablers offering those services.
2) When non-cash payment fraud occurs, there are direct economic costs. The PSD2[73] determines who bears these costs (i.e. the liability of the different actors), which, in most cases, is the enabler.
   In general, payment service providers bear the financial consequences which occur after the notification of lost, stolen or misappropriated payment instruments. Pursuant to article 70 of the PSD2, the payment service provider must ensure that appropriate means are available at all times, allowing the payment service user to notify the loss, theft or misappropriation of payment instruments.
   Card issuers are some of the enablers most affected by fraud. For example, when fraud takes place on less protected terminals in non-EU countries, most of the losses

[73] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

generated are on the card issuers' side due to a lack of specific settlements and regulations on the refund of losses caused by less safe terminals.
Credit card schemes (e.g. Visa, MasterCard) are also affected by fraud since they have to handle chargeback processes following fraudulent card transactions.
PSD2 also requires that payment service providers refund the totality of the economic losses to the payer, as long as the payer did not act with negligence[74] or fraudulently.

Payees

The payees, who get paid in exchange for a product or service, also suffer the consequences of non-cash payment fraud in two ways: through the loss of business opportunities due to lack of trust of the payers and through the direct losses caused by the fraud:

1) The payees (e.g. merchants) lose business opportunities when consumers are not willing to acquire their products and services due to lack of trust in the payment services.
2) Direct costs as a result of the fraud, e.g., when a service – such as a flight or train ticket – is provided against payment by credit card which is later blocked due to having been performed with stolen credentials.
   As indicated earlier, in the airline industry for example these costs are estimated at around USD 1 billion per year as a result of airline tickets purchased using compromised card data.[75]
   Other industries affected include accommodation and other travel services (e.g. car rental), as discussed in section 1.4.
   In terms of liability rules set by the PSD2, the payee is held liable when it fails to accept strong customer authentication.[76] Otherwise the payment service provider is the one liable.

It is difficult to determine which of the groups of stakeholders above is most affected by non-cash payment fraud. Whereas the payment service providers (i.e. the enablers) bear most of the liability according to the PSD2, the payers such a Bulgarian citizen who loses more than two thirds of his monthly wage, or the payees such as the airline industry which loses more than USD 1 billion per year due to card fraud, are also significantly affected.

1.5. What is the EU dimension of the problem

Non-cash payment fraud has a significant cross-border dimension, both within the EU and beyond.

[74] Pursuant to Article 69(1)(b) of the PSD2 'The payment service user entitled to use a payment instrument shall notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument'
[75] See also here
[76] Article 4(30) of the PSD2 defines strong customer authentication means as "an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data"

www.parlament.gv.at

For example, with regard to **card fraud,** whereas only a fraction of the transactions (<10% in value) are cross-border (within and outside SEPA), they account for half of the total fraud. The disproportion is particularly significant for transactions acquired from outside SEPA (2% in value), which account for 22% of all fraud. [77]

In a typical skimming case, the credentials of a credit card can be stolen in a Member State, the counterfeit card can be created in another Member State and the cashing out with the counterfeit card can occur in a country outside the EU without the same security standards (in particular EMV). Box 3 illustrates this point with a concrete example:

Box 3: the cross-border nature of non-cash payment fraud

In 2013, criminals from 27 countries around the world worked together to steal more than $45 Million in cash from ATMs, using counterfeit cards.

Criminals from Eastern Europe broke into the network of credit card processors in India and the United Arab Emirates, stealing prepaid card numbers and removing their withdrawal limits. They then used criminal networks to have counterfeited cards made with the stolen credentials and distributed the cards to hundreds of criminal groups around the world, who agreed on a date and time to hit simultaneously as many ATMs as possible. During the 10 hours that the joint robbery last, criminals carried out 36,000 ATM operations in 27 countries, walking away with over $45 Million in cash.[78]

In general, non-cash payment fraud has an increasing digital/online component, which reinforces its cross-border dimension.

See annex 5 (evaluation of the existing policy/legal framework) for a detailed analysis of the existing cross-border challenges to tackle these crimes.

1.6. How would the problem evolve, all things being equal

This section presents a series of quantitative estimates and qualitative considerations that describe how non-cash payment fraud could evolve in the coming years, all things being equal. These estimates and considerations inform the baseline policy option of doing nothing, which will be discussed in sections 4, 5 and 6.

Quantitative estimates

Since fraud data exists only for card fraud (the most important non-cash payment instrument in terms of number of transactions, see figure 3), the quantitative estimates will focus on it. As indicated in section 1.2.3. when assessing the magnitude of fraud, by considering only the available data of card fraud, the size of the problem is being underestimated. In the same way,

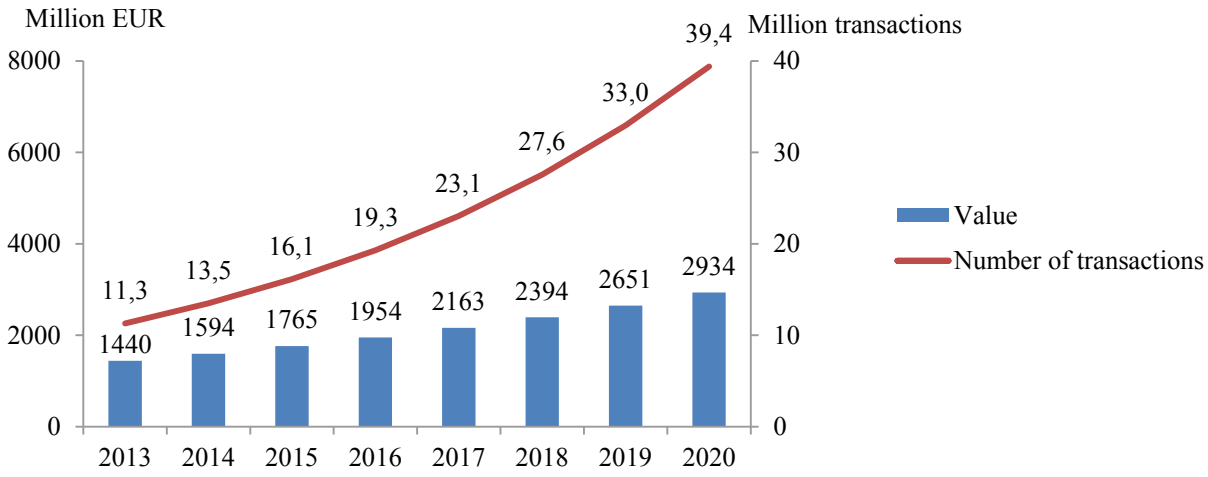
[77] European Central Bank, Fourth Report on Card Fraud, 2015
[78] See here for more information

www.parlament.gv.at

by using this data to quantitatively develop the baseline scenario, it is likely that the forecasts underestimate the magnitude of the problem.

As seen in section 1.2.3, the compounded annual growth rate of card fraud was 11% in terms of value and 20% in terms of number of transactions, over the 2011-2013 period. All things being equal, we could assume that these annual growth rates would continue in the coming years.[79] If so, the **value** of card fraud would **double** by 2020 compared to 2013, with almost **four times** as many fraudulent **transactions**:

Figure 9: estimated evolution of card fraud (2013-2020)



Qualitative considerations

The evolution of non-cash payment fraud is linked to the following factors:

1. Digitalisation of the economy.
   The exponential nature of the digital age not only brings exponential possibilities for economic growth but also for cybercrime, including those within non-cash payment fraud. The value of monetary damage caused by reported cybercrime is **50 times** higher now than it was in 2001, when the Framework Decision was adopted,[80] and is likely to continue growing.
   All things being equal, cybercrime will continue to generate important economic benefits for criminals, which justify the enormous amount of R&D hours required to produce malware, the main tool to carry out cybercrime (**every day**, more than 300,000 **new** malware samples are detected).[81]
   By 2020 it is expected that **50 billion** new devices (cars, homes, medical devices, buildings, mobile phones, dishwashers, toys…) will be connected to the Internet. This "Internet of Things" will generate massive amounts of information about its users, part of

[79] Estimates by The Nielsen Report indicate compounded annual growth rates of a similar order of magnitude for the value of card fraud globally for the 2011-2020 period (16%)
[80] Estimates based on cybercrime reported to the US Internet Crime Complaint Center (IC3), Statista, 2016
[81] As reported by Kaspersky Labs, 2014

which could be sensitive enough to be exploited by criminals to commit non-cash payment fraud.

2. Emergence of new payment instruments.
   The burst of innovation in the current technology revolution will likely continue developing new payment instruments to make the payment experience more convenient for users. Unfortunately, new payment instruments can also generate new opportunities for criminals. Furthermore, law enforcement may not be prepared to tackle them effectively (e.g. due to loopholes in the legal system or a lack of skills to deal with them).
   For example, new payment instruments could make use of **biometrics** as a way to identify the payer. Biometrics (e.g. fingerprints, palm prints, iris…), unlike passwords or credit card credentials, are permanent identification markers, so the consequences of them being stolen and misused can be more problematic for the victims.
   Other areas that could bring important innovations are **artificial intelligence** and **robotics.** These technologies have the potential to revolutionize the way non-cash payments are done by introducing increasing automation, governed by complex algorithms that could potentially be manipulated for fraudulent purposes.

3. Nature of the crime.
   As more and more countries join the technology revolution and more people around the world get connected to the Internet, the **cross-border** nature of non-cash payment fraud becomes even more relevant.

   Furthermore, Internet not only can provide training materials to commit fraud but also the necessary tools through the **crime-as-a-service** model.[82]

Box 4: carding websites as an example of crime-as-a-service

Carding websites and the actors operating behind them generally work through defined schemes.

Once the cards data have been stolen (e.g. through POS/ATM skimming or e-commerce/payment processors websites hacking), they are sold to brokers/resellers

[82] A business model that allows for the provision of cybercrime capabilities or ready to use cybercrime tools to other individuals or criminal groups.

who typically purchase them in bulk. These subjects, in turn, sell cards data to the so-called "carders", using marketplaces in the dark web.[83] Carders usually purchase them paying with bitcoins. [84]

Cards can be chosen according to their original zip codes so that criminals can reduce the risk of raising suspicions of the issuing bank when cashing them out. Many websites offer guarantees of the validity of the card and provide valid replacements in case the card is blocked before the carder manages to cash it out. Cards data are then either loaded in pre-paid cards in order to purchase in stores specific gift cards (e.g. Amazon gift cards) or they are used to manufacture counterfeit credit cards. [85]

More people connected unfortunately also means more potential fraudsters that could take advantage of those training materials and tools, likely at a **low risk**, due to the challenges to cross-border investigation and prosecution common to cybercrimes in general (e.g. attribution, access to digital evidence, jurisdiction).

Some existing EU instruments currently under transposition by Member States could contribute to reduce non-cash payment fraud to some extent:

- The PSD2 (to be transposed by January 2018) could reduce fraud thanks to its strong customer authentication requirements for remote transactions. At the same time, PSD2 also aims to facilitate the entry of new payment providers, which could lead to new forms of fraud.
- The Directive on the freezing and confiscation of instrumentalities and proceeds of crime[86] seeks to attack the financial incentive which drives crime, but aims mainly to ensure a minimum level of protection from criminal infiltration in the legal economy through the acquisition of assets and to facilitate the mutual recognition of freezing and confiscation orders in other Member States. This instrument alone would, however, not be sufficiently deterrent, as confiscation in general only occurs after a successful freezing of illicit assets following a conviction. Moreover, its deterrent effect will be limited if criminals are able to better hide their assets outside of the EU, resulting in a net capital flow of criminal money out of the EU.

These instruments, however, do not fully address the problem drivers identified specific to non-cash payment fraud, such as the lack of criminalisation of certain behaviours, obstacles to

[83] More information here
[84] Prices range from as little as $9 (for software generated cards) up to $100 per card, depending on the available information on the card (type of card, "base" , limits, etc.). Multiple cards can also be purchased in packages
[85] More information here
[86] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union

effective investigation and prosecution or prevention issues linked to information sharing gaps in public-private cooperation and lack of awareness of victims.

The baseline scenario would fall short in addressing concerns expressed by stakeholders, who indicated a strong consensus that the Framework Decision is not comprehensive, and that there are emerging trends that should be better covered. Also, a number of stakeholders (particularly private companies and trade, business or professional associations) agreed that it is necessary to have a more coherent level of penalties for offences related to non-cash means of payment across the EU. Most of them considered that different levels of penalties may result in different prioritisation of cases at national level, hampering cross-border cooperation and possibly creating "safe havens" for criminals. Stakeholders from the private sector (such as merchants and financial institutions) expressed frustration about the lack of legal certainty with regard to information sharing, which hampers cooperation with law enforcement authorities. The baseline scenario would leave this unchanged.

In summary, non-cash payment fraud is likely to increase in value, volume and complexity, all things equal.

1.7. Evaluation of the existing policy framework

The evaluation of the existing policy framework indicates that the Framework Decision is only partially relevant to the needs of stakeholders in the area of non-cash payment fraud.

Specifically, the scope of the Framework Decision is no longer fully relevant in view of recent technological developments, and provisions on cross-border cooperation and exchange of information do not seem to be aligned with the increasing international dimension of the crime, where multiple parties around the world may be involved, including both criminals and victims.

The results of the evaluation were identified as the problem drivers for non-cash payment fraud, presented in section 1.3.

Please see annex 5 for more details on the evaluation.

2. WHY SHOULD THE EU ACT

Legal basis

The legal basis for EU action is Article 83(1) of the Treaty on the Functioning of the European Union:

"The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly ***serious crime with a cross-border dimension*** *resulting from the nature or impact of such offences or from a special need to combat them on a common basis.*

www.parlament.gv.at

Article 83(1) explicitly mentions **counterfeiting of means of payment, computer crime and organised crime** as areas of particularly serious crimes with a cross-border dimension.

As discussed in the problem analysis in section 1, counterfeiting of means of payment is one type of non-cash payment fraud. Section 1 also explained how non-cash payment fraud has an increasing digital dimension which falls under computer crime. Furthermore, section 1 also described how non-cash payment fraud is part of organised crime.

Subsidiarity

Non-cash payment fraud has a very important cross-border dimension, both within the EU and beyond, as described in sections 1.3 (remember Hans' case, where as many as 10 Member States could be involved) and 1.5 (remember the real 2013 case of counterfeiting cards affecting 27 countries). Also, increasingly, these crimes are moving entirely online. The objective of effectively combating such crimes therefore cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way:

- As described in the previous section, these crimes create situations where the victim, the perpetrator and the evidence can all be under different national legal frameworks, within the EU and beyond. As a result, it can be very time consuming and challenging for single countries to effectively counter these criminal activities without common minimum rules.
- The need for EU action has already been acknowledged through the creation of the **existing EU legislation** on combating fraud and counterfeiting of non-cash means of payment (the Framework Decision).
- The need for EU intervention is also reflected in the current initiatives to coordinate Member States measures in this field at EU level, such as a dedicated **Europol** team working on payment fraud[87] and the **EMPACT Policy Cycle priority** on operational cooperation against non-cash payment fraud.[88] The added value of these initiatives in helping Member States combatting these crimes was acknowledged multiple times during the stakeholder consultation, in particular during the expert meetings.

Another added value of EU action is to facilitate cooperation with non-EU countries, given that the international dimension of non-cash payment fraud frequently goes beyond EU borders. The existence of minimum common rules in the EU can also inspire effective legislative solutions in non-EU countries thereby facilitating cross-border cooperation globally.

3. WHAT SHOULD BE ACHIEVED

This section identifies the general and strategic objectives for a possible EU intervention to address the gaps identified in section 1.

[87] See Europol's website
[88] More information here

www.parlament.gv.at

1.8. General policy objectives

There are two general policy objectives, which describe the ultimately intended goals of a possible EU intervention (i.e. reducing the negative impact of the consequences of non-cash payment fraud identified in section 1.4):

1) **Enhance security,** the main general objective, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore as an enabler of other criminal activities, including terrorism.

2) **Support the digital single market,** by reducing the negative impact on economic activity that non-cash payment fraud causes to the different stakeholders (section 1.5). This includes both losses derived from the reduced trust of consumers and businesses in the payment processes as well as direct losses.

These objectives are interrelated:

- Synergies: enhancing security would support the digital single market, as the economic losses caused by non-cash payment fraud would decrease. It would also reduce the risk of consumers and businesses of falling victim of fraud, increasing their trust and therefore economic activity.
- Trade-offs: enhancing security could entail additional costs and constraints to the digital single market. For example, the implementation of increased security in payment authentication systems could bring additional costs to businesses, which could have a negative impact in their operations, in particular for SMEs. In addition, consumers might actually be less willing to use payment services if they find the security measures too burdensome.

1.9. Specific policy objectives

There are three specific policy objectives:

1) Ensure that a **clear, robust and technology neutral** policy/legal framework is in place.
2) Eliminate **operational obstacles** that hamper investigation and prosecution.
3) Enhance **prevention.**

These objectives address the problem drivers identified in section 1.3:

Table 2: problem drivers, specific objectives and general objectives

www.parlament.gv.at

Problem drivers	Specific objectives	General objectives
⇨ Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised	1) Ensure that a **clear, robust and technology neutral** policy/legal framework is in place	1) Enhance **security** 2) Support the **digital single market**
⇨ **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised		
⇨ Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States		
⇨ Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution		
⇨ It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution	2) Eliminate **operational obstacles** that hamper investigation and prosecution	
⇨ Under-reporting to law enforcement due to constraints in **public-private cooperation** hampers effective investigations and prosecutions		
⇨ **Information sharing gaps** in **public-private cooperation** hamper prevention	3) Enhance **prevention**	
⇨ Criminals exploit the **lack of awareness** of victims		

These objectives will be monitored through a series of indicators described in section 7, which also specifies possible data sources, whether the information is already being collected and the actors responsible for collecting it.

1.10. Consistency with other EU policies and objectives

The general and specific objectives identified are consistent and complementary with those of other EU policies and legislation:

The Treaties

The previously mentioned objectives are consistent with:

- the Treaty on European Union[89], which, on Article 3.2, establishes that "the Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of people is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime."

[89] Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012

- the Treaty on the Functioning of the European Union, which, on Article 67.3 establishes that the Union should "endeavour to ensure a high level of security through measures to prevent and combat crime, […], and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws".

The Charter of Fundamental Rights of the European Union[90]

The objectives of a possible initiative would be consistent with the Charter of Fundamental Rights, in particular:

- Right to liberty and security (Article 6 of the Charter), as this would be the main objective of the initiative;
- Protection of personal data (Article 8), with which potential provisions on exchange of information, etc… should comply;
- Freedom to conduct a business (Article 16), since the initiative would aim to enhance protection of businesses bearing the consequences of fraud;
- Consumer protection (Article 38) and right to an effective remedy and to a fair trial (Article 47), since the initiative would aim to enhance protection of and assistance to consumers that become victims of fraud.

Security and Digital Single Market strategies

The main general objective, enhancing security, is at the core of the EU Agenda on Security and the EU Cybersecurity Strategy:

- The EU Agenda on Security sets out the principles for EU action to respond effectively to security threats by 1) preventing terrorism and countering radicalisation; 2) fighting organised crime; 3) fighting cybercrime.

  One of the actions described for the period 2015-2020 is “reviewing and possibly extending legislation on combating non-cash fraud and counterfeiting by including new forms of crime against financial instruments".

  In the 6th progress report towards an effective and genuine Security Union[91], the European Commission confirms that, "concerning payment card fraud, it is necessary to widen existing law enforcement cooperation to a broader range of criminal activities which target non-cash means of payments."

[90] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407
[91] Report from the Commission to the European Parliament and the Council - Sixth progress report towards an effective and genuine Security Union, COM(2017) 213 final

The 7th progress report[92] highlights a number of legislative and non-legislative initiatives in the field of crime prevention, which could contribute to the objectives of a possible EU action, such as:

- increasing the role of Europol as an EU hub for information exchange on serious cross-border crime, in order to become more effective, efficient and accountable;
- building Member States' capacities for cybercrime resilience and implementing the Network Information Security (NIS) Directive;
- improving the access to electronic evidence to investigators in cross-border cases.

In March 2017, the Council decided to continue the EU Policy Cycle[93] for organised and serious international crime for the period 2018-2021, based on the 2017 EU Serious and Organised Crime Threat Assessment "Crime in the Age of Technology" (SOCTA 2017)[94]. The SOCTA 2017 provides an overview of the most important criminal threats in the EU, which should be tackled as priorities, and which include payment card fraud.

- The EU Cybersecurity Strategy aims at creating the world's most secure online environment in the EU, including for online payment transactions, an aim which is fully aligned with the main general objective of enhancing security.

- The Digital Single Market Strategy identifies existing key challenges that need to be overcome to ensure better access to digital goods and services across Europe. These challenges include providing adequate protection to consumers and businesses' assets and tackling cybercrime through the adoption and implementation of a strong and effective legislation. The general objective of supporting the digital single market is obviously aligned with this Strategy.

EU legislative context

As described in section 1.1. (policy context), various EU legislative acts have been adopted since the Framework Decision entered into force, both in criminal and civil law. The general and specific objectives of a possible new EU action on combatting non-cash payment fraud would be consistent with these legislative acts:

1. Pan-European **cooperation mechanisms in criminal matters** that facilitate coordination of investigation and prosecution (procedural criminal law):
    - Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States;
    - Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union;

[92] Communication from the Commission to the European Parliament, the European Council and the Council - Seventh progress report towards an effective and genuine Security Union, COM(2017) 261 final
[93] Draft Council Conclusions on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021
[94] EU Serious and Organised Crime Threat Assessment, Europol 2017

- Directive 2014/41/EU regarding the European Investigation Order in criminal matters;
- Council Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties;
- Council Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings;
- Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States;
- Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime;
- Council conclusions on improving criminal justice in cyberspace;
- Regulation (EU) 2016/794 on Europol;
- Council Decision 2002/187/JHA setting up Eurojust.

The general and specific objectives are fully aligned with those of these legislative acts. As a principle, the potential new intervention would not introduce provisions specific to non-cash payment fraud that would deviate from these horizontal instruments, to avoid fragmentation which could complicate the transposition and implementation by Member States.

The only possible exception could be the support and protection of victims, which the proposed EU action could complement. Directive 2012/29/EU establishes minimum standards, which could be completed for the area of non-cash payment fraud, if needed. For example, this Directive only covers natural person, whereas legal persons can also become victims of non-cash payment fraud, as discussed in section 1.4 (who is affected and how). Also, this Directive focuses on providing assistance in the context of criminal proceedings. A new initiative would aim at providing assistance to victims outside the criminal proceeding (for instance as regards to consequences relating to identity theft).

In the case of the European Arrest Warrant and the European Investigation Order, the new initiative would also be consistent with both, by setting up an appropriate level of minimum maximum sanctions that reflects the gravity of the crime and therefore ensures that the EAW and is applicable and the EIO can be recognised and executed for the defined offences.

2. Legal acts that **criminalise conduct** related to fraud and counterfeiting of non-cash means of payment (substantive criminal law):
    - Directive 2013/40/EU on attacks against information systems:
        - A new initiative would be complementary to Directive 2013/40, by addressing a different aspect of cybercrime.[95] The two instruments would correspond to

[95] The EU Cybersecurity Strategy indicates that "cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a

different sets of provisions of the Council of Europe Budapest Convention on Cybercrime,[96] which represents the international legal framework of reference for the EU.[97]

- The initiative would also be consistent with Directive 2013/40, as it would be based on the same approach regarding specific issues (e.g. defining minimum maximum levels of penalties, jurisdiction).

- Directive 2014/62/EU on the protection of the euro and other currencies against counterfeiting by criminal law:
  - A new initiative would be complementary to Directive 2014/62/EU as it would cover counterfeiting of non-cash payment instruments, while Directive 2014/62/EU covers the counterfeiting of cash.
  - It would also be consistent with Directive 2014/62/EU, as it would use the same approach on some provisions such as on investigative tools.
- Directive 2017/541/EU on combating terrorism:
  - A new initiative would be complementary to Directive 2017/541/EU, as it would aim to reduce the overall amount of funds derived from non-cash payment fraud, most of which go to organized crime groups to commit serious crimes, including terrorism.
- The Proposal for a Directive on countering money laundering by criminal law:
  - The new initiative and the proposal for a Directive on countering money laundering by criminal law are complementary as the latter provides the necessary legal framework to counter the laundering of criminal proceeds generated by non-cash payment fraud ("money mules") as a predicate offence.

3. Legal acts that regulate the payment process, in particular to **facilitate secure payments** across the EU:
   - Revised Payment Services Directive (PSD2):
     - A new initiative on non-cash payment fraud would be complementary to PSD2, as it would aim at reducing crime, while PSD2 enhances payments security. Also, it would enable public-private cooperation and enhance reporting to law enforcement authorities, which would complement statistical data provided under the PSD2.
   - Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, (the fourth Anti-Money Laundering Directive):

---

primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."

[96] Council of Europe Convention on Cybercrime (ETS No.185). Directive 2013/40 corresponds to Articles 2 to 6 of the Convention, whereas a new initiative would correspond to Articles 7 and 8 of the Convention

[97] Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT

- A new initiative would be complementary to Directive 2015/849, as it would address the situation where the non-cash payment instruments have been, for instance, unlawfully appropriated, counterfeited or falsified by the criminals, whereas Directive 2015/849 covers the situation where criminals abuse non-cash payment instruments with a view to concealing their activities.

- Proposal for a Directive amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing:[98]
  - A new initiative would be consistent with the proposal for a Directive amending Directive 2015/849 as it incorporates the same definition of virtual currencies. If this definition changes during the adoption process, the definition in the new initiative should be aligned accordingly.
- Regulation (EU) 2015/847 on information accompanying transfers of funds, regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive):
  - A new initiative on non-cash payment fraud would be complementary to these legislative acts, as it would aim at reducing crime, while these acts enhance payments security.

In addition to the above legislative acts, the new initiative would be coherent with the General Data Protection Regulation and the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data:

- The new data protection legislation modernises the already existing rules on security of personal data. In addition, the new legislation (GDPR) imposes an obligation of a notification of personal data breaches to the national data protection supervisory authorities and to the data subject in certain circumstances. Non-compliance with such rules will be subject to administrative fines.
- A new initiative on non-cash payment fraud would be in compliance with the GDPR and Directive (EU) 2016/680, as it would:
  - pursue the objective of greater protection of personal data (credit card number shall be considered as personal data and, credit card also contains other personal data such as the name of a citizen).

[98] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC

- leave to Member States to take the necessary measures to favour public-private cooperation, including exchange of information, while providing for these measures to be in compliance with the GDPR.

4. WHAT ARE THE VARIOUS OPTIONS TO ACHIEVE THE OBJECTIVES

This section addresses the possible policy options for achieving the objectives defined in section 3 and tackling the problems identified in section 1. Each **policy option** is made of a group of **policy measures.**

The following process was applied to determine the **policy options**:

1) **mapping** of policy **measures**,
2) **analysis** of policy **measures**: identify which policy **measures** to retain and which to discard,
3) **formation** of policy **options**: combine retained policy **measures** into groups to form the policy **options.** The options are cumulative (i.e. increasing level of EU legislative action), as it will be detailed in section 4.3.

1.1. Mapping of policy measures

Three broad possibilities were considered in the analysis: do nothing, do not legislate (i.e. support through non-legislative tools) or legislate. Figure 10 maps the policy measures (1 to 14) for each of these possibilities and the policy options (A to D) in which the measures could be grouped:

Figure 10: mapping of policy measures and policy options

www.parlament.gv.at

1.2. Analysis of policy measures

1.2.1. Policy measures retained

The policies measures retained are those that provide the alternatives that are most feasible (legally, technically and politically), coherent with other EU instruments, effective, relevant and proportional to tackle the problem drivers detected in section 1:

Table 3: problem drivers identified and corresponding policy measures retained

Problem drivers	Policy measures retained
Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised.	1, 3
Preparatory acts for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised.	1, 5, 11
Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States.	1, 5
Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution**.**	1, 7, 8, 9
It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution and assistance to victims.	1, 12
Under-reporting to law enforcement due to information sharing gaps in **public-private cooperation** hampers investigations and assistance to victims.	2, 14
Criminals exploit the **lack of awareness** of victims.	1, 14

1.2.2. Policy measures discarded

- Possible solution to the problem of certain crimes not being effectively prosecuted because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised.

  Policy measure 4 considers adding detailed definitions with a comprehensive list of payment instruments and forms of crime.

  Compared to policy measure 3 (technology-neutral definitions), this measure would be less effective in covering non-cash payment instruments and crimes that could arise in the next years, with the risk of becoming outdated in a short time. Furthermore, it would create issues of consistency with the existing EU legal framework, especially with the definition of payment instruments included in the Payment Services Directive. This would also lead to significant administrative costs in transposing the specific definitions at national level, since most of the Member States have already adopted the definition in the Payment Services Directive.

www.parlament.gv.at

- Possible solution to the problem of **preparatory acts** not being effectively prosecuted because they are criminalised differently in Member States or not criminalised.

  Policy measure 6 considers including preparatory acts as an aggravating circumstance to sanctions, and sets minimum level of maximum penalties for the criminalised offences.

  Compared to measure 5 of criminalising preparatory acts, this measure could entail less administrative and financial costs for law enforcement, especially in Member States that apply the principle of legality[99], because preparatory or supportive activities would be investigated and taken into account as an aggravating circumstance to sanctions only if the fraud actually occurred. For the same reason, however, it would be much less effective in preventing and fighting the different forms of non-cash payment fraud, since law enforcement would act only after the actual fraud occurred.

- Possible solution to the problem of **victims** not always receiving adequate assistance.

  Policy measure 10 considers adding new provisions protecting natural persons from identity theft, in coherence with the Victims' Directive.

  Compared to measure 11 of adding new provisions protecting natural and legal persons, this measure only covers a limited group of victims. In particular, it leaves out SME's, which, by lacking the resources of larger companies, are more vulnerable to fraud and its negative consequences. Although this option would entail less administrative and financial costs for law enforcement and Member States, these costs would likely be outweighed by the negative impact on consumption and trade flows that lower trust in non-cash payment transactions brings if an important group of victims remains not properly covered.

- Possible solution to the problem of **under-reporting** to law enforcement.

  Policy measure 13 considers including provisions on **mandatory reporting** to law-enforcement.

  Compared to measure 14 on encouraging reporting, mandatory reporting could be more effective in increasing the chances of detecting, prosecuting and sanctioning perpetrators, since a much higher number of cases would be reported to law enforcement and more information would be available for investigations. However, these benefits are likely to be outweighed by the dramatic increase of the administrative and financial costs borne by law enforcement agencies to be able to deal with the dramatic increase in the volume of information (not all of which would be useful), especially in those Member States applying the principle of legality. The private sector would also incur in important administrative costs to put in place the mechanisms for systematic reporting.

[99] In a legality system, public prosecutors don't have the discretion to cancel the prosecution of a crime, which is possible in countries where the principle of opportunity is applied.

Encouraging reporting is likely to be a proportionate measure that could generate more positive results in practice.

In addition to these measures discarded during the analysis, some other alternatives were early discarded:

- Full harmonisation of level of penalties (minimum and maximum levels).
  This alternative is not feasible in EU criminal law, which can only introduce minimum rules on sanctions.
- Creating an EU database on fraud data.
  This idea seemed attractive in theory as a possible way for private sector to cooperate with law enforcement and facilitate investigations. However, there would be many different technical and legal challenges for the creation of such database (e.g. data protection/retention issues, etc).

1.3. Policy options

The retained policy **measures** were grouped in different ways to form the policy **options**.

The basic criterion to form a policy option was that it should tackle **all** the problems detected in the evaluation. After trying multiple combinations of the retained measures, with alternative policy approaches and alternative policy instruments (e.g. self-regulation, non-regulation, regulation), and taking into account the input from stakeholders (e.g. with regard to the importance of jurisdiction), four policy options were selected for further analysis.

The options are **cumulative,** i.e. with an increasing level of EU legislative action. Given that the issue at hand is basically a **regulatory failure**, it is important to lay out the full range of regulatory tools to determine the most proportionate EU response.

The table below shows the intervention by summarizing how each of the policy options tackle all the problems detected and help achieve the specific objectives:

www.parlament.gv.at

Table 4: problem drivers, specific objectives and options (intervention logic)

<table>
<tr><th colspan="2">Problem drivers</th><th colspan="2">Specific objectives</th><th colspan="4">Options</th></tr>
<tr><th colspan="2"></th><th colspan="2"></th><th>A</th><th>B</th><th>C</th><th>D</th></tr>
<tr><td colspan="2">⇨ Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular non-corporeal) are criminalised differently in Member States or not criminalised.</td><td colspan="2" rowspan="4">1) Ensure that a clear, robust and technology neutral policy/legal framework is in place.</td><td rowspan="6">Implementation of existing EU law, exchange of best practices</td><td colspan="3" rowspan="3">Provisions in new Directive including:
• technology neutral definitions
• preparatory acts
• minimum level of penalties
• jurisdiction (competence) rules as in the Attacks Against Information Systems Directive</td></tr>
<tr><td colspan="2">⇨ Preparatory acts for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised.</td></tr>
<tr><td colspan="2">⇨ Cross-border investigations can be hampered because the same offences are sanctioned with different levels of penalties across Member States.</td></tr>
<tr><td colspan="2">⇨ Deficiencies in allocating jurisdiction can hinder effective cross-border investigation and prosecution.</td><td>Provisions in new Directive complementing EIO and injunction rules</td></tr>
<tr><td colspan="2">⇨ It can take too much time to provide information in cross-border cooperation requests, hampering investigation and prosecution.</td><td colspan="2" rowspan="3">2) Eliminate operational obstacles that hamper investigation and prosecution</td><td colspan="3">Provisions in new Directive to facilitate effective cross-border cooperation</td></tr>
<tr><td colspan="2">⇨ Under-reporting to law enforcement due to constraints in public-private cooperation hampers effective investigations and prosecutions.</td><td colspan="2" rowspan="2">Facilitate self-regulation for public-private cooperation</td><td colspan="2" rowspan="3">Provisions in new Directive on:
• encouraging reporting
• information sharing
• awareness raising</td></tr>
<tr><td colspan="2">⇨ Information sharing gaps in public-private cooperation hamper prevention.</td><td rowspan="2">3) Enhance prevention</td></tr>
<tr><td colspan="2">⇨ Criminals exploit the lack of awareness of victims.</td><td colspan="2">Implementation of existing EU law, exchange of best practices</td></tr>
</table>

www.parlament.gv.at

1.3.1. Option O: baseline

As seen in section 1.6, non-cash payment fraud is likely to increase in value, volume and complexity, all things equal, and in particular under the current policy and legal framework.

The problem drivers previously identified would evolve based on separate initiatives in Member States rather than being mitigated through a specific and common EU approach.

Please refer to section 1.6 for a complete description of the baseline scenario.

1.3.2. Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation

Compared to the baseline situation, this option would not only focus on the implementation of existing relevant legislation (e.g. the Framework Decision, PSD2, Directive on Attacks Against Information Systems), but also on trying to address the problem drivers through exchanges of best practices and capability building.

Specific actions would include:

- publication of a third implementation report on the Framework Decision alongside a guidebook explaining the legislative framework in each Member State, highlighting best practices to law enforcement and other stakeholders to facilitate cooperation;
- specific activities promoted by the Commission (e.g. guidelines, training courses, workshop events with country representatives and exchange of good practice and experiences) for ensuring that the provisions of the Framework Decision and of the complementary EU legislation are utilised to their fullest extent.

In addition, it would include a self-regulatory framework for public-private cooperation between relevant actors from the financial services industry, law enforcement and other stakeholders (e.g. merchants), aiming to improve the exchange of information, which could in turn improve investigation and prosecution and prevention.

The Commission could incentivise the creation of such public-private partnership through a dedicated Communication.

Improvements in public-private cooperation would need to be addressed with the current tools, through the exchange of best practices. Successful examples of public-private cooperation already exist in a number of Member States[100] to facilitate reporting of fraud to

[100] The study " Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combatting fraud in and counterfeiting of non-cash means of payment" analysed a number of national public-private cooperation initiatives, which can be considered as examples of best practices:

- France: FIA-NET, Phishing initiative, Groupement des Cartes Bancaires (CB), and French LEA.
- Germany: the German Cybercrime Competence Centre (G4C);
- Italy: the platform OF2CEN, CertFin;

www.parlament.gv.at

law enforcement authorities and step up response to identified threats. These can provide guidelines about how to improve public-private cooperation.

With regard to the awareness raising activities, the Commission would facilitate the exchange of best practices among Member States. These activities could target any of the types of victims of non-cash payment fraud described in section 1.4. ("Who is affected and how").

1.3.3. Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation

Compared to the baseline, this option introduces a new basic legislative framework covering:

- **technology neutral definitions**, to ensure that fraud can be effectively prosecuted regardless of the payment instrument used. To reinforce the future proof aspect of the definitions, they should be drafted in a way that encourages investments in security technologies. One way to do this is to maintain the part of the definition of payment instrument in the Framework Decision that specifies that the instrument should be secured.[101] As recital 10 of the Framework Decision explains:

  "By giving protection by penal law primarily to payment instruments that are provided with a special form of protection against imitation or abuse, the intention is to encourage operators to provide that protection to payment instruments issued by them, and thereby to add an element of prevention to the instrument";

- **preparatory acts**, covered as a separate offence and regardless of whether the payment fraud has occurred or whether it has generated financial losses for the victim; it also includes provisions criminalizing **identify theft** as an aggravating circumstance;

- minimum maximum **level of penalties**, to ensure that different level of penalties across Member States do not hamper cross-border investigations. Other EU legislative acts in criminal law have set minimum levels of maximum penalties, such as the Directive 2013/40 on attacks against information systems, Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography, among others. In the area of fraud, the European Parliament has made explicit its support to establishing minimum level of criminal sanctions "to ensure a degree of consistency across the EU on sanctions concerning financial fraud. Such a step, would in the view of the Committees, also discourage forum shopping on the part of money-launderers and fraudsters."[102]

- The Netherlands: ECTF (Electronic Crime Task Force);
- Slovakia: Slovakian Banking Association Commission for security of payment cards;
- The UK: the Dedicated Card and Payment Crime Unit (DCPCU), Cyber information Security Partnership (CiSP), Action Fraud, Financial Fraud Action, National Cyber Security Center (NCSC)

[101] Article 1(a) of the Framework Decision defines payment instrument as "a corporeal instrument… which is protected against imitation or fraudulent use, for example through design, coding or signature;"

[102] Protection of the Union's Financial Interests (PIF Directive), Legislative Train Schedule, European Parliament

www.parlament.gv.at

As discussed in section 1.3.1(c), the experts shared conflicting views concerning the effectiveness of minimum maximum sanctions, but there was consensus as to their usefulness to be coherent with other EU legislative acts. Indeed, this option would be fully coherent with minimum maximum sanctions in related EU legislation.

- facilitation of **cross-border cooperation**, for example by:
  - strengthening and clarifying the role of the dedicated contact points.[103]
  - encouraging Member States to share information with Europol.
  - collecting statistics on investigations and prosecutions of non-cash payment fraud offences.
- **jurisdiction** provisions on competence would be updated as in the Attacks Against Information Systems Directive.[104]

Idem to option A, the Commission would:

- support non-legislative initiatives to foster **public-private cooperation** through a self-regulated framework, which would address both the under-reporting and the information sharing gaps;
- address the **lack of awareness** of victims by facilitating the exchange of best practices and ensuring the full implementation of existing and relevant EU law.

A technology neutral definition covering all forms of value transfer would ensure that all forms of crime relating to payment instruments are tackled.

The criminalisation of preparatory acts would allow the investigation of conduct that enables non-cash payment fraud. It could also imply a more effective use of investigative resources, since it would make possible the investigation of cases before they become too complex (e.g. before the credentials are sold to multiple parties that use them to actually commit the fraud). The criminalisation of preparatory acts could also have a deterrent effect for this offence and for fraud itself.

Whereas law enforcement and judicial authorities by and large consider national penalties appropriate, other stakeholders (particularly private enterprises, trade, business or professional associations) underline that it is necessary to have more coherent level of penalties for offences related to non-cash means of payment across the EU to avoid different prioritisation of cases at national level, hampering cross-border cooperation and creating "safe havens" for criminals. This option would therefore address these concerns by setting a minimum level for maximum penalties.

[103] Stakeholders from both the private and the public sectors raised the need for clearly identified dedicated contact points.
[104] In addition, there will be full alignment with the ongoing work on improving criminal justice in cyberspace (i.e. without introducing specific cases applicable only to non-cash payment fraud).

www.parlament.gv.at

To avoid that unclear rules on jurisdiction result in cases not being prosecuted, this option would set clearer criteria to mitigate the risks of conflicts of jurisdiction.

Cross-border cooperation would benefit from further approximation of national legal frameworks. Moreover, additional measures aiming at clarifying the role of contact points in law enforcement and reducing response times would further favour effective cooperation. This would address the concerns raised by law enforcement agencies in the open public consultation, as well as the concerns raised in the expert meetings organised by the Commission.

Furthermore, this option aims at increasing the protection of the interests of the victims by defining as aggravating circumstances situations in which fraud has consequences going beyond the financial loss (e.g. reputational or psychological damage resulting from identity theft).

1.3.4. Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness

Compared to the baseline, this option introduces the same new basic legislative framework described in option B (i.e. with new provisions on **definitions, preparatory acts, level of penalties and cross-border cooperation**), as well as the same provisions on **jurisdiction** as in option B (i.e. update on competence as in AAIS Directive).

Differently from option B, this option would:

- address the issues related to **public-private cooperation** (under-reporting and information sharing for prevention) through new provisions on **encouraging reporting**; Whereas in option B the issue of information sharing gaps in public-private cooperation would be addressed through self-regulation, in option C the Directive would include provisions requiring Member States to ensure that appropriate reporting channels are made available and that they remove the obstacles to an effective exchange of information between private entities and public authorities such as law enforcement. The main difference between self-regulation and encouraging reporting is therefore that the latter involves legislation and the former doesn't.

  During the stakeholder consultation, private entities pointed out that they frequently chose not to report incidents due to legal uncertainty in the exchange of information and that with legal certainty these incidents would have been reported. The provisions on encouraging reporting could address this issue.

- address the **lack of awareness** by introducing specific provisions ensuring awareness raising among potential victims. The Directive would not detail what these specific awareness raising measures should be, as it would be up to the Member States to

www.parlament.gv.at

decide the concrete measures that would be most effective and efficient, considering the national situation.

In addition to the requirements on Member States to ensure that a clear, robust and technology neutral policy/legal framework is in place this option would introduce requirements for Member States to address the legal obstacles that may hamper information exchange by providing the legal certainty that stakeholders from private sector consistently asked for during the consultations.

1.3.5. Option D: same as option C but with additional jurisdiction provisions complementing EIO and injunction rules

This option is the same as option C but adding to its jurisdiction provisions other measures that facilitate the cross-border exchange of evidence for investigations and prosecutions by:

- complementing the European Investigation Order (EIO)[105] with measures adapted to non-cash payment fraud, such as:
  - providing adequate training on investigative techniques;
  - ensuring the protection of exchanged data (also when personal data is shared) and that information disclosed is proportionate to the purpose for which it was requested and that the information was acquired in accordance with the relevant legislative, regulatory, or administrative provisions;
  - having the issuing authority provide feedback to the executing authority about the use made of the evidence provided and about the outcome of the prosecution.

  As discussed in the policy context in section 1.1., the EIO updates the legal framework applicable to the gathering and transfer of evidence between Member States, based on mutual recognition of judicial decisions.

- adapting the rules on injunctions (orders granted by a court or an administrative body whereby someone is required to perform or to refrain from performing a specific action) for cooperation/evidence purposes, by:
  - including rules to enable Member States to issue injunction orders for co-operation (for example injunction for cessation of an infringement) whenever there is a jurisdictional implication and interest to have a legal standing in a foreign court ruling;

[105] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

www.parlament.gv.at

- including an obligation for Member States to maintain a central database of the injunctions for cooperation initiated on their territory that would allow for monitoring the enforcement of these orders;
- strengthening the procedural law provisions in respect to measures safeguarding the victims' rights in a foreign jurisdiction and adopting provisional measures for securing the enforcement of the judgment (i.e. freezing injunctions[106]).

In addition to the requirements on Member States described in option C, this option would include additional rules on jurisdiction to facilitate access to information by law enforcement.

5. WHAT ARE THE IMPACTS OF THE DIFFERENT POLICY OPTIONS

The following criteria were used to assess the impacts of each policy option:

Table 5: criteria for the assessment of options

Criteria	Rationale for the assessment
Coherence	**Internal coherence** with the strategic objectives of the intervention**:** • **Enhance security,** by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism • **Support the digital single market,** by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud
	External coherence with relevant, existing EU legislation
Effectiveness	**Social** impact: • Intermediate: o increased law enforcement capacity to address criminal activity relating to new forms of non-cash payment fraud; o increased capacity to investigate, prosecute, and sanction criminals; o decreased number of criminal acts and organised crime gains relating to new forms of non-cash payment fraud; o increased protection for victims of non-cash payment fraud; o stronger cooperation between public institutions/private sector • Aggregated impact: enhanced **security**

[106] A freezing injunction is a court order which prevents a party from disposing of or dealing with its assets

www.parlament.gv.at

	Economic impact: • Intermediate: o increased consumption and trade flows due to higher trust of consumers in digital purchases of goods and services; o increased consumer choice due to reduction of fraud; o reduced costs for economic operators (i.e. financial services providers, retail goods/services providers) that are victims of fraud • Aggregated impact: support of the **digital single market**
Efficiency	Financial and administrative **costs**: one-off and continuous costs for public and private sectors
	Simplification benefits for businesses/citizens, and for national/regional/local administrations
Fundamental rights	• Right to liberty and security; • Personal data protection; • Freedom to conduct business; • Consumer protection; • Right to effective remedy, in particular the remedies available before the courts The assessment takes into account the consequences of identity theft, such as reputational damage and costs to rectify the consequences of the theft (e.g. replacing identity documents; rectification of negative entries in victims' credit history)
EU added value	Description of additional benefits resulting from EU intervention compared to what could be achieved by Member States only

The effectiveness criterion was split into social and economic impacts, which were in turn divided into intermediate impacts, to increase the granularity and detail of the assessment.

Better Regulation guidelines (2015) require an assessment of **environmental impacts**. The evaluation results did not indicate any implications of the Framework Decision for environment and in the assessment of environmental impacts of the policy options were not considered significant.

The criteria above were used to assess the impacts of each policy option qualitatively and quantitatively.

1.4. Qualitative assessment

The methodology used in the qualitative assessment was the following:

1. Qualitatively assess each policy measure using the above criteria (see annex 4).
2. Qualitatively assess the policy options, taking into account the assessment of the policy measures they are made of (see annex 4).
3. Provide scores to grade the policy options and enable their comparison (see section 6). The scoring system used was the following:

Table 6: scoring system for qualitative assessment of options

www.parlament.gv.at

Score	Impact level
+2.5 to +3.0	Highly positive (e.g. the option is likely to result in substantial cost savings for firms, much better protection of victims, much broader investigation and prosecution capacity, etc)
+1.5 to +2.0	Moderate positive (e.g. high cost savings, better protection of victims, broader investigation and prosecution capacity, etc)
+1	Small positive (e.g. uncertain or indirect impact)
-0.5 to +0.5	Very uncertain or insignificant
-1	Small negative
-2 to -1.5	Moderate negative
-3 to -2.5	Highly negative

Limitations:

The **qualitative assessment of impacts** of different policy measures and options has been carried out against the baseline constituted by evaluation findings and available data. Where these were not available, the assessment is based on plausible explanations on if and how the situation is likely to change under a particular scenario (e.g. if and how introducing a definition of payment instruments and a broad definition of crimes will affect rights to liberty and security: small positive impact can be expected as forms of non-cash payment not covered by current legislation will be regulated and this improves chances for prosecuting fraud criminals and protection of victims of fraud crimes). However, such judgements can be subjective. To mitigate this limitation, the judgements and justifications of the scores were validated with focus group participants and external reviewers.

The following sections summarize the social, economic and fundamental rights impacts described in detail in annex 4.

5.1.1. Social impact

0. Baseline

The increasing number of criminal acts and organised crime gains are likely to have moderate negative impact on security.

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation

www.parlament.gv.at

Improved cooperation between public and private sectors and capacity to address non-cash payment fraud, together with enforced prosecution could lead to small improvements of security.

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation

Given the lack of binding measures addressing the rights of non-cash payment fraud' victims (i.e. identity theft related) and the cooperation between public and private sectors, a moderate impact is expected in terms of the improvement of security, mostly due to the increased chances of detecting, prosecuting and sanctioning criminals.

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness

A significant impact is expected in terms of the improvement of security, due to the increased chances of detecting, prosecuting and sanctioning criminals, the enhanced protection of fraud' victims from identify theft and the facilitation of public-private cooperation, including reporting.

Option D: same as option C but with jurisdiction provisions complementing EIO and injunction rules

This option will increase the chances for detecting, prosecuting and sanctioning criminals by building on existing law enforcement cooperation mechanisms, i.e. the EIO and the injunctions for cooperation.

5.1.2. Economic impact

0. Baseline

Non-cash payment transactions will increasingly contribute to the digital single market by facilitating digital purchases of goods and services. However, the growing level of fraud and its costs, borne by consumers and economic operators, is likely to remain a barrier for the digital single market to achieve its full potential.

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation

The level of fraud and its cost for individual consumers and economic operators is likely to be somewhat compensated by increased consumption and the overall impact on functioning of the digital market and competition could be small and negative. This, coupled with additional administrative and financial costs to support the implementation of existing EU legislation, the exchange of best practices and capability building, would likely have moderate negative impact on the digital single market.

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation

Accumulated benefits of consumptions, trade flows, consumer choice and cost savings for economic operators would likely drive significant positive impacts on the functioning of the digital market and competition. However, the economic benefits would be mitigated by increased administrative and financial costs.

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness.

Accumulated benefits of consumer choice and protection (both natural and legal persons), consumption (both business-to-customer and business-to-business), and cost savings for economic operators would likely drive significant positive impacts on functioning of the digital market and competition. However, the economic benefits would be mitigated by increased administrative and financial costs.

Option D: same as option C but with jurisdiction provisions complementing EIO and injunction rules.

Idem as option C, but with higher administrative and financial costs, which would result in a lower positive economic impact.

5.1.3. Fundamental rights impact

0. Baseline

The Framework Decision does not explicitly refer to protection of personal data, which is instead currently covered by Directive 95/46/EC. This Directive will be repealed in 2018 by the General Data Protection Regulation, which will provide a single set of rules and modernise data protection across the EU.[107]

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation

There would be no additional impact on fundamental rights, provided that the establishment of self-regulation for public-private cooperation is done in full compliance of the EU data protection rules.

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation

[107] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

www.parlament.gv.at

This option could have a positive impact on the right to security by regulating forms of non-cash payment fraud not covered currently. Also, the criminalisation of preparatory acts could have a positive impact on the protection of personal data.

As in option A, attention to existing data protection rules should be given when facilitating self-regulation of public-private partnerships and any new legislative framework shall be designed to fully comply with the legislation on the protection of personal data.

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness

In addition to the applicable considerations made for option B, attention should be given to the provisions encouraging reporting, to ensure that they respect data protection rules.

The new provisions on raising awareness could have a positive impact on the right to security.

Option D: same as option C but with jurisdiction provisions complementing EIO and injunction rules

In addition to the applicable considerations made for option C, the additional tools for investigation and prosecution that it provides (complementary rules to the EIO and injunctions) should be implemented in full respect of the data protection legislation.

5.2. Quantitative assessment

The quantitative assessment aims at estimating for each policy option:

- the main **financial and administrative costs**, distinguishing between one-off and continuous costs;
- the main **benefits** (savings) due to reduction of fraud and reduction of organised crime gains.

Costs

The following costs were estimated, using a number of assumptions:

- One-off costs:
  - Transposing EU legislation in Member States.

  Assumptions:
    - Civil servant daily wage of € 130, based on the average monthly earnings for the public administration by Eurostat, which is about € 2 600,[108] and assuming 20 working days in a month.
    - Using as a reference the data from a related impact assessment,[109] it was assumed that 20 working days are necessary for transposing into national

[108] Civil servants remuneration, Eurostat
[109] Study for an impact assessment on a proposal for a new legal framework on identity theft, 2012, p160

www.parlament.gv.at

law "simple" EU legislation, and 60 working days are necessary for transposing "more articulated" EU legislation.

- Continuous costs:
  - Implementing and enforcing the new legislation, in particular when it leads to an increase in the number of cases to be investigated.
  - Facilitating cross-border cooperation, including collection of statistics, operation of contact points (also for reporting purposes) and cooperation with Europol and Eurojust.
  - Implementation of awareness raising campaigns.

  Assumptions:
  - Civil servant daily wage of € 130, as described above.
  - While there is little firm basis for the number of days required to complete the continuous costs estimates, for the only purpose of comparing the policy options it was assumed as a reference that a Member State requires around 100 working days per year for implementing "simple" legislation and around 200 working days for more complex legislation. This reference was also used to estimate the cross-border cooperation costs and implementation of awareness raising campaigns.

A general assumption was that the estimated cost of each **policy option** was the **sum** of the estimated costs of the **policy measures** it is made of. This could lead to an overestimation of the costs, since some economies can occur when developing/transposing legislation combining two or more legislative and/or non-legislative measures.

Limitations:

- The quantification of the main costs of the policy measures/policy options is limited by the lack of data, which requires the use of a number of assumptions.
- In particular, with regard to reporting for private entities, it would be voluntary, so it is not possible to provide meaningful estimates of their potential reporting costs.
- These assumptions have a certain degree of approximation and subjectivity, mitigated by relying on the findings of the qualitative assessment, which were validated with focus groups and external reviewers.

The tables below summarize the one-off and continuous costs estimates for the retained policy measures and the policy options they combine into:

Table 7: one-off and continuous costs estimates for the retained policy measures (EUR)

POLICY MEASURES	ONE-OFF COSTS	CONTINUOUS (ANNUAL) COSTS
1	€ 0	€ 0
2	€ 0	€ 0
3	€ 70,200	€ 526,500
5	€ 210,600	€ 689,000
7	€ 70,200	€ 44,720

8	€ 70,200	€ 351,000
9	€ 70,200	€ 351,000
11	€ 70,200	€ 702,000
12	€ 70,200	€ 252,720
14	€ 70,200	€ 70,200

Table 8: one-off and continuous costs estimates for the policy options (EUR)

POLICY OPTIONS	ONE-OFF COSTS	CONTINUOUS (ANNUAL) COSTS
O	€ 0	€ 0
A (measures 1+2)	€ 0	€ 0
B (2+3+5+7+12)	€ 421,200	€ 1,512,940
C (3+5+7+11+12+14)	€ 561,600	€ 2,285,140
D (3+5+7+8+9+11+12+14)	€ 702,000	€ 2,987,140

Annex 4 contains the complete details of the calculations, as well as the one-off and continuous costs for the EU institutions (e.g. development of legislation, facilitating best practices, etc…).

Benefits

The main benefit that would be expected of initiatives combatting non-cash payment fraud is a reduction of it.

Assumptions:

- To estimate how each policy option could reduce fraud, it was assumed that the reduction of fraud would be proportional to the decrease of criminal acts and organized crime gains related to non-cash payment fraud, which was qualitatively assessed for each of the policy measures.
- The qualitative scores range from -2 (policy measure 0) to +2 (policy measure 5).
- In the baseline (policy measure 0), it was assumed that there will not be any decrease of criminal acts and organized crime gains (0%).
- The range of qualitative scores for the policy measures was converted into a range of percentages using taking into account the above and with an equivalence of 1 to 1. In other words:

Percentage decrease of criminal acts = -2 – qualitative score

www.parlament.gv.at

The qualitative scores range of -2 to +2 results in a respective range of 0% to -4% change (decrease) of criminal acts and organized crime gains resulting from non-cash payment fraud.

- The percentage for each policy option was the sum of the percentages for its policy measures.
- It is assumed a current level of fraud of 1.44 billion EUR, which corresponds to the level of card fraud in 2013 calculated by the European Central Bank (latest data available).

Limitations:

- As in the case of costs, the quantification of the benefits is limited by the lack of data, which requires the use of a number of assumptions:
    - The lack of data concerns the total volume of fraud. Taking the 2013 data of card fraud from the 2015 ECB report as basis to estimate the potential benefits will likely lead to an underestimation of the benefits. As discussed in section 1.2.30., although card fraud appears to be the main form of non-cash payment fraud (~ 75% in value), there are others (e.g. cheques, virtual currencies, mobile payments), in which the policy options would likely also generate benefits.
- The lack of data also affects the capacity to estimate the benefits in general. In the absence of indicators to monitor the reduction of fraud, this can only be estimated through a number of assumptions, which have a certain degree of approximation and subjectivity, mitigated by relying on the findings of the qualitative assessment, which were validated with focus groups and external reviewers.
- In particular, the assumptions of the conversion of the qualitative range into percentages of decrease of fraud were used for the sole purpose of comparing the options. Therefore, the total value of benefits for a given policy option must be interpreted in relation to the other options, rather than as an accurate estimate of the actual reduction of fraud that a given policy option would cause.

The tables below summarize the benefits for the retained policy measures and the policy options they combine into:

Table 9: estimated benefits for the retained policy measures (EUR million)

POLICY MEASURES	Qualitative scores for decreasing number of criminal acts	Percentage estimate of decreasing number of criminal acts	Fraud reduction	Remaining value of fraud
0	-2.0	0.0%	€ 0.0	€ 1,440
1	-1.0	-1.0%	€ 14.4	€ 1,426
2	-1.0	-1.0%	€ 14.4	€ 1,426
3	-1.0	-1.0%	€ 14.4	€ 1,426
5	2.0	-4.0%	€ 57.6	€ 1,382

www.parlament.gv.at

7	-0.5	-1.5%	€ 21.6	€ 1,418
8	-1.0	-1.0%	€ 14.4	€ 1,426
9	-1.0	-1.0%	€ 14.4	€ 1,426
11	-2.0	0.0%	€ 0.0	€ 1,440
12	-1.0	-1.0%	€ 14.4	€ 1,426
14	0.5	-2.5%	€ 36.0	€ 1,404

Table 10: estimated benefits for the policy options (EUR million)

POLICY OPTIONS	Total percentage estimate of decreasing number of criminal acts	Total fraud reduction	Total value of fraud
O	0.00%	€ 0	€ 1,440
A (measures 1+2)	-2.00%	€ 29	€ 1,411
B (2+3+5+7+12)	-8.50%	€ 122	€ 1,318
C (3+5+7+11+12+14)	-10.00%	€ 144	€ 1,296
D (3+5+7+8+9+11+12+14)	-12.00%	€ 173	€ 1,267

5.3. REFIT potential

Qualitative

The qualitative assessment described earlier has taken into account the simplification potential of the different policy options compared to the Framework Decision, in the analysis of efficiency impacts.

For example, the simplification potential includes:

- Further approximation of national criminal law frameworks (e.g. by providing common definitions and a common minimum level of sanctions for the maximum penalty) would simplify and facilitate cooperation between national law enforcement agencies investigating and prosecuting cross-border cases.
- In particular, clearer rules on jurisdiction, a reinforced stronger role for national contact points and the sharing of data and information between national police

www.parlament.gv.at

authorities and with Europol could further simplify the procedures and practices for cooperation.

Quantitative

The REFIT potential of the policy options can only be assessed from a qualitative point of view.

It is not possible to quantify these costs and benefits beyond those already estimated for the impacts of the legislative initiative of the preferred option due to a lack of data (and in some cases the impossibility to isolate the effects of the Framework Decision). In particular, it was not possible to conduct a systematic backward-looking analysis of the existing costs.

It is important to stress that, overall, the REFIT potential of this initiative is very limited:

1. Firstly, the 2001 Framework Decision is already a relatively simple legal act with limited potential to be further simplified.

2. Secondly, this initiative aims to increase security by addressing the current gaps. This would normally entail more administrative costs to investigate and prosecute crimes that are not currently covered, rather than significant savings that would result from simplifying cross-border cooperation.

3. Thirdly, the initiative does not aim to impose additional legal obligations on businesses and citizens, but to request Member States to encourage and facilitate reporting through appropriate channels (rather than imposing mandatory reporting), in line with other EU instruments such as Directive 2011/93 on combatting the sexual abuse and sexual exploitation of children and child pornography (Art. 16(2))

It would be interesting to assess the REFIT potential of the set of EU measures to combat terrorist financing, of which an initiative on combatting non-cash payment fraud would be part of. That broader analysis was out of the scope of this impact assessment.

6. HOW DO THE OPTIONS COMPARE

5.4. Comparison of options

This section compares the options using the qualitative and quantitative analysis of impacts from section 5.

Qualitative comparison

The table below shows the qualitative scores for each main assessment criteria and each option, based on the previous assessment of impacts.
The overall score was determined as the average of the scores of the main assessment criteria, (i.e. taking all criteria into account equally) in order to obtain the best, well-rounded option.

www.parlament.gv.at

As discussed in section 5.1, the judgements and justifications of the scores were validated with focus group participants and external reviewers:

Table 11: comparative qualitative assessment of the policy options

		O	A	B	C	D
Coherence	Internal	0	1	2	2.5	3
	External	0.5	1	2	2	-2
Effectiveness	Social	-0.5	1	2	2.5	3
	Economic	-1.5	-1	2	2.5	3
Efficiency	Costs	0	-1	-1.5	-2	-3
	Benefits	0	-0.5	1	1.5	2
Fundamental rights		0	0	1.5	2	2
EU added value		0	0.5	1.5	2.5	3
Overall score		**-0.2**	**0.1**	**1.2**	**1.7**	**1.4**

Coherence

On the basis of the outcome of the evaluation (annex 5), the relevance of the existing legal framework appears to be questionable. Also, very few respondents to the consultation indicated that the existing legal EU legal framework sufficiently addressed the different issues concerning non-cash payment fraud, such as the definitions of payment instruments, criminalisation of preparatory acts or the lack of common minimum level of penalties. Therefore, options including legislative initiatives (B, C and D) are considered preferable to the baseline scenario and to option A which includes non-legislative measures only.

Most of the stakeholders consider the level of public-private cooperation to not be fully effective in combating non-cash payment fraud. Private sector representatives appear to be most dissatisfied. Main obstacles in cooperation include, for instance, limitations in the possibility to share information with law enforcement authorities and in the use of tools to enable the exchange of information. The vast majority of stakeholders[110] agreed that in order to investigate and prosecute criminals, financial institutions should be allowed to spontaneously share with the national police or the police of another EU country some of the victim's personal information (e.g. name, bank account, address, etc.).
Therefore, options including measures to increase legal certainty for exchanging information were preferred.

As regards to the coherence with other legislative instruments, law enforcement and judicial authorities' representatives highlighted the value of making the definition of payment

[110] Open public consultation feedback: general public

www.parlament.gv.at

instruments consistent with the one included in the Payment Services Directive (PSD2) and pointed out the need to take into account relevant provisions under the Directive 2013/40 on Attacks Against Information Systems. At the second expert meeting, law enforcement and judicial authorities' representatives agreed on the possibility of replicating, *mutatis mutandis*, the provisions on jurisdiction included in the Directive 2013/40.
Option D would possibly interfere with the ongoing process on access to electronic evidence. This process aims at providing a comprehensive set of solutions that would address the identified issues regarding the territoriality of investigations across the board (and not for a specific crime area, as it would be the case if option D was pursued).

Effectiveness

If the current situation remains unchanged, consumer choice may decrease because of higher risks of being victims of fraud, the costs for economic operators could increase due to better protection needed against new forms of crime and the number of criminal acts and organised crime gains could continue rising, bringing about a negative effect in terms of effectiveness of EU action.

In option A, addressing the problem drivers by improving implementation of existing EU legislation, including by promoting the exchange of best practices and capability building, could improve the conditions for investigations and prosecutions to a certain extent. It is uncertain that these initiatives would be able to help evolve the national legal frameworks to address in a timely manner new means of payment and offences related to non-cash payment fraud that are currently not covered (e.g. sale of stolen credentials). It would also be difficult to achieve a common minimum level of penalties through only the initiatives of this option. Finally, it is unlikely that this option would effectively tackle the jurisdiction issues, given the current gaps in the Framework Decision, as illustrated through specific cases presented by Europol in the expert meetings.

The level of effectiveness of law enforcement action could raise significantly for options including legislative measures (B, C, D): while option A would not likely bring about overall improvements in efficiency, option B would increase the chances of detecting, investigating, prosecuting and sanctioning conduct that enable non-cash payment fraud (preparatory acts) as discussed earlier.

Poor cooperation among private and public authorities was mentioned by several stakeholders[111] as obstacles encountered when fighting non-cash payment fraud. Legislative measures (C, D) to enhance public-private cooperation and exchange of information, were considered more effective than non-legislative ones (A, B). However, the non-mandatory nature of envisaged legislative solutions reduces the differences between options, in terms of effectiveness.

[111] Open public consultation feedback from international or national public authority, private enterprises, Professional consultancy, law firm, self-employed consultant, Trade, business or professional association and other categories

www.parlament.gv.at

The expected effects of a self-regulatory framework for public-private cooperation in options A and B would be positively influenced by: 1) the extended scope of the revised legislation, which ensures that cooperation would also tackle new payment instruments and forms of crime; 2) the facilitated cross-border cooperation, making it easier for these initiatives to involve stakeholders from different Member States and better tackle cross-border fraud.
However, possible legal issues regarding the ability to exchange information would not be addressed.

Efficiency

The baseline scenario would not bring about any cost, or benefit. Under option A, where possible actions would not be of a legislative nature, additional costs related to implementation would be limited to those Member States that still need to bring their national legislation fully in line with the related EU legislation. Awareness raising to enhance prevention would have limited costs, as it is the case for workshops and other actions devoted to the exchange of best practices. Costs of implementation and enforcement of new legislation would naturally increase, as legal requirements augment; for instance, measures aiming at enhancing cross-border cooperation through points of contact in law enforcement or a provision on collecting statistics would have continuous financial consequences for national administrations.

On the other hand, benefits would equally increase for options including legislative measures: approximation of national criminal law frameworks, through common definitions and minimum levels of maximum penalties set at EU level would ease cooperation.

Fundamental rights

Non-regulatory solutions would have no impact on fundamental rights, while options B, C and D would have a positive impact as regards to the right to liberty and security and data protection.

EU added value

The magnitude of the added value of the EU intervention under option A is likely to be limited compared to the baseline: it is unclear how effective this action would be in incentivising voluntary public-private cooperation agreements. In addition, given that a number of such agreements already exist, the added value of the communication is likely to be quite limited. On the other hand, this option would not affect the competences of the Member States.

Legislative measures would represent an added value compared to the Framework Decision. For example, a common minimum level of sanctions would reduce the disparities between Member States and ensure a more coherent treatment of fraud criminals across the EU. Also, with regard to cross-border cooperation, Member States would be unlikely to cooperate effectively without EU action.

www.parlament.gv.at

The introduction of legislative measures would add a new layer of interference in the competences of the Member States. As options B, C and D increase respectively the number of legislative measures, they also increase respectively the degree of interference with the competences of the Member States.

The table below summarizes the pros and cons of the different policy options:

Table 12: summary of pros and cons of the policy options

Options	Pros	Cons
O	• No additional costs.	• No change in the definitions of payment instruments and offences would not bring any improvement in law enforcement action. Non-cash payment fraud would continue growing, and with it the risk of falling victim of it, as well as prevention costs and the gains for organised crime groups, with negative effects on security and economic development.

www.parlament.gv.at

		• Public-private cooperation would continue at today's levels.
A	• Little additional costs	• This option would likely have little impact on the criminal law framework, and therefore limited impact on improving investigations and prosecutions. • It fails to address properly the need for enhanced prevention. • The effectiveness of non-legislative measures is unclear.
B	• Approximation of criminal law frameworks would: A) ease cooperation B) increase the chances of detecting, investigating, prosecuting and sanctioning conduct that enable non-cash payment fraud. C) allow for tackling strategically the main enabling factors for crime. • Expected positive economic impacts including on the digital single market.	• It fails to address properly the need for enhanced prevention and public-private cooperation. • Divergences in interpretation among Member States remain possible, due to broad definitions.
C	• Idem option B. • In general, it effectively pursues the two general objectives of EU intervention.	• Divergences in interpretation among Member States remain possible, due to broad definitions Reporting on voluntary basis would not guarantee a dramatic increase in the number of information (fraud incidents and/or suspicious transactions) collected by law enforcement authorities. • Significant financial and administrative costs (€ 2.7 million) to EU institutions and national authorities.
D	• Increased law enforcement effectiveness	• Lack of coherence with other ongoing processes (e.g. on improving criminal justice in cyberspace)

The policy options meet the specific objectives to different degrees:

1) Ensure that a clear, robust and technology neutral legal framework is in place

As outlined in the evaluation of the existing policy and legislative framework (annex 5), the Framework Decision appears to be outdated and to fall short in addressing some of the areas that are considered key for countering non-cash payment fraud effectively.

Option A would provide elements of clarification and marginally increase approximation of national legislation (by bringing Member States that still need to make progress in certain areas in line with the Framework Decision).

www.parlament.gv.at

However, the Framework Decision does not contain a **technology neutral** definition and stakeholders agreed that it needs improvement as regards to the criminalisation of specific preparatory acts. Options B, C and D would address those issues, by updating definitions (e.g. payment instruments, payment orders and information systems) to make them **technology neutral** and therefore **future proof**, while being as precise as criminal law requires. These technology neutral definitions will be used to describe the offences to be criminalised and ensure that the legal framework allows that all the relevant crimes to be effectively investigated and prosecuted (as explained in section 1.3. the problem drivers indicate that the issue at hand is mostly a **regulatory failure,** where the current EU legislative framework has become partially obsolete, due mainly **to technological developments).**

A clear and robust legal framework governing exchange of information is also needed to enable public-private cooperation, as clearly pointed out by representatives of the private sector. Options A and B would address this issue only partially, without a providing a clear legal basis for exchange of information, like the one provided in options C and D.

2) Eliminate operational obstacles that hamper investigation and prosecution

Option A aims at addressing obstacles to investigation and prosecution through training and exchange of best practices. Although these can be valid supporting measures, they are likely to bring only marginal improvements to cooperation, compared to providing a clear role for national points of contact and clarifying rules on jurisdiction to avoid conflicts of jurisdiction (as in the cases presented by Europol and included in annex 5 as an example), as options B, C and D would provide.

Moreover, timely access to information and effective information exchange with private parties have been identified as key issues by experts. By providing legal certainty, options C and D would pave the way towards public-private cooperation, creating the conditions for enhancing the quality of reporting and the possibility for private parties to assist better law enforcement authorities in their action.

3) Enhance prevention

Under options A and B, enhancing prevention would be an indirect consequence of the improvements in public-private cooperation brought about by non-legislative initiatives.

However, possible legal issues regarding the ability to exchange information would not be addressed, failing to meet stakeholders' expectations, as expressed in particular by the private sector in the expert meetings and by other stakeholders (e.g. national banking federation) in the open public consultation.

Therefore, prevention would be more effective if a sound framework for public-private cooperation is in place, as proposed under options C and D.

Qualitative comparison

www.parlament.gv.at

The table below compares the estimated costs and benefits for the different options

Table 13: comparative quantitative assessment of the policy options (EUR million)

	O	**A**	**B**	**C**	**D**
Overall costs	0	0	1.9	2.8	3.7
Overall benefits (savings)	0	- 28.8	- 122.4	- 144.0	- 172.8
Total (savings)	**0**	**-28.8**	**-120.5**	**-141.2**	**-169.1**

As highlighted in section 5.2 (quantitative assessment), given the limitations caused by the lack of data, the calculation of benefits was carried for the main purpose of comparing the options. In consequence, the total value of benefits must be interpreted in relation to the other options, rather than as an accurate estimate of the actual reduction of fraud that the preferred policy option would actually cause. In particular, the much higher potential benefits in relation to the costs for options B, C, D should not be taken at face value. That said, option D is the option that could offer comparatively more benefits in the form of reduction of fraud, followed closely by option C.

5.5. Preferred option

On the basis of the assessment, the preferred option identified is **option C**.

Option D scores slightly better than C against several assessment criteria (such as social and economic impacts) but C has a better overall qualitative score. Option C is the second best option in terms of potential savings, but given the limitations in the quantitative assessment due to lack of data, more weigh was given to the qualitative assessment to decide on the preferred option.

Main advantages

Option C would effectively pursue the strategic objectives of the EU intervention since:

- broad minimum common definitions (measure 3) and minimum rules for sanctions (measure 5) would address different forms of fraud, including new and emerging ones, cross-border crimes (measures 12 and 7), and preparatory activities (measure 5);
- assistance to victims (measure 11) would further reinforce consumers' trust and economic operators in non-cash payment transactions and the digital single market.

In particular, option C would incorporate technology neutral definitions, which are more likely to be future proof. To further reinforce the future proof aspect, the definitions would be drafted in a way that encourages investments in security technologies, by, for example, specifying that the payment instrument is provided with a protection against imitation or abuse (i.e. is secured).

www.parlament.gv.at

Furthermore, the liability rules set by the PSD2, in which the payment service provider is the one liable unless the payee fails to accept strong customer authentication, also contribute to encouraging payment service providers to ensure an up to date level of protection of the payment instrument.

The expected economic impacts in terms of a) consumer choice and protection (both individuals and businesses), b) consumptions (both business-to-customer and business-to-business), and c) cost savings for economic operators are likely to drive significant positive impacts on the functioning of the digital single market.

The EU added value of the option can be associated to the provisions a) setting minimum levels of sanctions (which could reduce the disparities between Member States and to ensure a more coherent treatment of fraud criminals across EU), and b) facilitating cross-border cooperation.

Main disadvantages

The use of broad and all-encompassing definitions for non-cash payment instruments and crimes could lead to divergences in interpretation across Member Stats, possibly limiting the simplification benefits.

Reporting on voluntary basis would not guarantee a dramatic increase in the number of information (fraud incidents and/or suspicious transactions) collected by law enforcement authorities. However, information (including modi operandi and other strategic information) could be shared by the private sectors within established public-private cooperation mechanisms, provided that partners' liabilities and responsibilities will be addressed and defined.

The option would entail significant financial and administrative costs (one-off of EUR 0.56 million and annual costs of 2.28 million EUR) to national authorities for transposing, implementing and enforcing the new legislation, facilitating cross-border cooperation, including collection of statistics, operation of contact points (also for reporting purposes) and cooperation with Europol and Eurojust, as well as implementation of awareness raising campaigns.

Trade-offs

This option would enhance security but at a cost for national administrations.

Also, the implementation of increased security in payment authentication systems could generate constraints for consumers which may affect negatively their willingness to engage in online payments and the digital single market (e.g. if consumers find the security measures too burdensome).

Fundamental rights

www.parlament.gv.at

As described in section 5.1.3. (fundamental rights), the preferred option could have a positive impact on the right to security, freedom to conduct a business and consumer protection by regulating forms of non-cash payment fraud not covered currently.

The measures of this option have as final objective the protection of the rights of victims and potential victims. The establishment of a clear legal framework for law enforcement and judicial authorities to act upon criminal activities directly affecting the personal data of the victims, including the criminalisation of preparatory acts, may in particular have a positive impact on the protection of victims' and potential victims' right to privacy and right to protection of personal data.

At the same time, this option respects fundamental rights and freedoms as recognised by the Charter of Fundamental Rights of the European Union, and would have to be implemented accordingly. Any limitation on the exercise of such fundamental rights and freedoms would be subject to the conditions set out in Article 52(1) of the Charter, namely be subject to the principle of proportionality with respect to the legitimate aim of genuinely meeting objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, be provided for by law and respect the essence of those rights and freedoms.

In particular, this option respects the principle of legality and proportionality of criminal offences and penalties as, in providing for minimum rules on the criminalisation of non-cash payment fraud, it limits the scope of the offences to what is necessary to allow for the effective prosecution of acts that pose a particular threat to security and introduces minimum rules on the level of sanctions in accordance with the principle of proportionality, having regard to the nature of the offence.

The criminalization of preparatory acts could have a positive impact on the protection of personal data. That said, attention should be given to the provisions encouraging reporting, to ensure that they are in accordance with the fundamental right to protection of personal data and existing applicable legislation, including in the context of public-private cooperation.

Subsidiarity

Given the international dimension and the scope of the problems to solve, the measures included in the preferred policy options need to be adopted at EU level in order to achieve the identified objectives. In particular, action by Member States would fall short in addressing, e.g. the following issues:

- Differences among different definitions of criminal offences and level of sanctions among Member States, in order to enhance cross-border cooperation and ensure coherence in the law enforcement approach to non-cash payment fraud;
- Disparities about the protection of EU consumers and economic operators, therefore reinforcing trust in the digital single market and preventing deviations in their choices and buying behaviours;
- Obstacles to cross-border cooperation on combatting non-cash payment fraud.

www.parlament.gv.at

In addition, the preferred option offers the most added value at a reasonable degree of interference in the competences of the Member States.

Proportionality

Regulation has been discarded as delivery instrument of the policy option because Article 83(1) TFEU only allows for the means of Directives to give Member States a high degree of flexibility in terms of implementation.

The option would introduce a minimum set of common broad definitions, minimum level of maximum sanctions and rights of victims. Therefore, Member States would retain a degree of discretion in setting the levels of sanctions. Likewise, Member States would be allowed to grant more favourable rights to the victims of non-cash payment fraud.

The option would not impose disproportionate obligations to the private sectors (including SMEs) and citizens, since reporting to law enforcement authorities would be voluntary.

The costs that the preferred option would entail are justified in light of the negative consequences of non-cash payment fraud. As discussed in section 1.2.4. ("Why is it a problem"), at least EUR 1.4 billion per year are stolen to fund organized crime groups and activities such as terrorism, drug trafficking and trafficking in human beings. In addition, citizens and businesses suffer direct economic losses, representing an obstacle to the digital single market.

On the whole, the option does not go beyond what is necessary to achieve the objective identified for the EU intervention.

7. HOW WOULD ACTUAL IMPACTS BE MONITORED AND EVALUATED

The Commission should review the implementation of any (legislative or non-legislative) proposal on non-cash payment fraud with regard to the achievement of policy objectives identified in this impact assessment. A commitment to evaluating the impacts of a legislative act, if proposed, should be included in the draft text. This evaluation should be engaged 6 years after the deadline for implementation of the legislative act to ensure that there is a sufficiently long period to evaluate the effects of the initiative after it has been fully implemented across all Member States. It may include a public consultation and/or survey stakeholders to review the effect of the potential legislative act on the different categories of stakeholders.

In addition to that formal evaluation, the Commission will remain in close contact with the Member States and with the relevant stakeholders to monitor the effects of the new legislative act. The European multidisciplinary platform against criminal threats (EMPACT), part of the EU Policy Cycle,[112] represents an excellent forum to exchange of information with the Member States (law enforcement) and to gather first-hand information and qualitative

[112] More information here

www.parlament.gv.at

evidence on cross-border cooperation on combatting non-cash payment fraud. Qualitative evidence provided by law enforcement and prosecutors (e.g. examples of cases that cannot be prosecuted because jurisdiction cannot be established) can be a cost effective yet informative way to illustrate the gaps that a possible legislative instrument would aim to cover.
The Commission will also remain in contact with social partners such as victims' and consumers' associations.

The Commission should also submit a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the legislative act, 2 years after the deadline to implement it.

Table 14 summarizes the indicators proposed to monitor the achievement of policy objectives identified in this impact assessment. The general and specific objectives are the same ones as those proposed in section 3, whereas the operational objectives are linked to the preferred option described in section 7.2.

The indicator "Volume (value and number of transactions) of non-cash payment fraud" serves the two general policy objectives. It uses as sources the statistical data on fraud related to the different means of payment (not only cards) that payment service providers will be required to provide under Art.96(6) of PSD2 on incident reporting. Therefore, this indicator will provide additional information on the breakdown of fraud by non-cash means of payment, which will allow the future success of the intervention to be measured more broadly than only in terms of card fraud. In addition, the European Central Bank is currently devising definitions that would allow tracking fraud committed using different non-cash means of payment, and which will provide further data for this indicator.

To avoid putting any additional administrative burden on Member States or the private sector due to the collection of information used for monitoring, the proposed indicators mainly rely on the existing data sources (e.g. ECB, Eurobarometer).

The preferred option contains a requirement for Member States to collect national statistics on non-cash payment fraud crimes, to facilitate cross-border cooperation. This data will be used to monitor the ratio between fraud volume and law enforcement action. The costs of this data collection were included in the analysis of the options.

For the remaining data that is not currently available, the Commission will conduct a targeted survey. The costs of the survey should be borne by the Directorate General of Migration and Home Affairs within its operational expenditure (e.g. as support expenditure for operations of the Cybercrime policy area). The survey will be biannual and will be conducted at least twice, coinciding, if applicable, with the reporting requirements for the Commission on the transposition and implementation of the potential legislative act.
As a result, the proposed monitoring arrangements would not generate additional administrative burden (reporting obligations) for firms, including SMEs, beyond those already imposed by the reporting requirements on non-cash payment fraud data of Art. 96(6) of the PSD2.

www.parlament.gv.at

As seen throughout the Impact Assessment, the PSD2 is of key importance for the impact and the success of a potential legislative proposal on non-cash payment fraud because of the reporting requirements but also in multiple other areas such as prevention. Other EU policies and legislative instruments, such as the ongoing process on improving criminal justice in cyberspace, also have an impact on the success of the potential legislative act (see annex 6).

The benchmark against which progress will be measured is the baseline situation when the legislative act enters into force. The Commission will compile the necessary data at that point, conducting a small survey/study if necessary, funded by the Directorate General of Migration and Home Affairs.

With regard to targets (a proxy for success criteria), given the different situations in the Member States as the evaluation section describes (see annex 5), it was considered more effective to measure progress of each Member State against its own baseline, rather than through identical targets across Member States.

www.parlament.gv.at

Table 14: monitoring of general, specific and operational objectives

	Objectives	Monitoring indicators	Sources of data and/or collection methods	Data collected already?	Actors responsible for data collection
General	Enhance **security**	Volume (value and number of transactions) of non-cash payment fraud	ECB, EBA: data partly collected under Art. 96(6) of PSD2	Yes (ECB)	ECB, EBA (consolidation), Member States (collection)
		Profits for organized crime groups derived from non-cash payment fraud	Law enforcement agencies; e.g. contributions to Europol's threat assessment reports	Yes	Europol
	Support the **digital single market**	Volume (value and number of transactions) of non-cash payment fraud	ECB, EBA: data partly collected under Art. 96(6) of PSD2	Yes (ECB)	ECB, EBA (consolidation), Member States (collection)
		Trust of consumers	Eurobarometer: survey	Yes	European Commission
Specific	Ensure that a **clear, robust and technology neutral** policy/legal framework is in place.	Ratio between fraud volume and law enforcement action	Member States: annual data on investigations/prosecutions/ convictions	No	European Commission (consolidation), Member States (collection)
		Qualitative evidence of cases that cannot be prosecuted because the behaviour is not considered criminal	Police and judicial authorities: participation in the relevant EMPACT priority of the EU Policy Cycle	Yes	Europol, Eurojust and European Commission (consolidation), Member States (collection)
		Qualitative evidence of cases that cannot be prosecuted because jurisdiction cannot be established			
	Enhance **cooperation** to facilitate investigation and prosecution	Qualitative evidence of cases that cannot be investigated due to lack of cooperation			
		Qualitative evidence of cases that cannot be prosecuted because the information is not available			
	Enhance **prevention**	Number of structured public-private cooperation mechanisms established and number of entities involved	Member States: survey	No	European Commission
		Awareness of consumers and economic operators on risks and possibilities to address them	Eurobarometer: survey	Yes	European Commission
Operational	Enhance **cross-border operational cooperation**	Number of national contact points set up in accordance with the preferred policy option	Member States: survey	No	European Commission
		Number of relevant SIENA messages exchanged	Europol	Yes	Europol
		Number of cross-border operations under the relevant EMPACT priority	European Commission: participation in EMPACT	Yes	European Commission

www.parlament.gv.at

ANNEX 1: PROCEDURAL INFORMATION

1. Organisation and timing

The Directorate-General for Migration and Home Affairs (HOME) is the lead service for the preparation of the initiative (2016/HOME/077 – inception impact assessment published in May 2016) and the work on the evaluation and impact assessment.

Given that evidence was already available on difficulties encountered by law enforcement (see section 1.3. "Evidence", below) in tackling non-cash payment fraud, the decision was taken to run the evaluation of the current situation at the same time with the impact assessment. The results of the evaluation (presented in Annex 7) by-and-large confirm the preliminary analysis.

The evaluation of the current situation was carried out back-to-back with the Impact Assessment for possible new measures in the area of non-cash payment fraud. The Commission committed in the European Agenda of Security (2015) to review the existing legislation on combatting fraud and counterfeiting of non-cash means of payment. President Juncker reiterated that commitment by including improved rules on fraud in non-cash payments in his September 2015 Letter of Intent, initially planned for delivery in 2016. The proposal was rescheduled for delivery after the summer of 2017, which required carrying out the evaluation back-to-back with the Impact Assessment.

An inter-service steering group (ISSG), chaired by the Secretariat-General, was set up in December 2015 with the participation of the following Commission Directorates-General: Legal Service; Competition (COMP); Financial Stability, Financial Services and Capital Markets Union (FISMA); Informatics (DIGIT); Internal Market, Industry, Entrepreneurship and SMEs (GROW); Environment; Communications Networks, Content and Technology (CONNECT); Joint Research Centre (JRC); Justice and Consumers (JUST).

Invitations were also sent to DG Economic and Financial Affairs (ECFIN).

The ISG met three times, discussing the inception impact assessment, the terms of reference for the external study[113], the questionnaire for the public consultation, as well as subsequent reports of the support study and the draft impact assessment.

2. Consultation of the RSB

The Regulatory Scrutiny Board received the draft version of the present impact assessment report on 22 June 2017. It issued an impact assessment quality checklist on 7 July 2017 with a number of very helpful comments. A detailed response to the RSB quality checklist was sent in advance to the RSB meeting on 12 July 2017, which specified how each of the RSB comments would be incorporated to the final version of the impact assessment.

[113] Study available in the EU Bookshop.

www.parlament.gv.at

The RSB issued a positive opinion without reservations on 14 July 2017, with a number of recommendations that completed the previously issued quality checklist. All of the RSB comments were incorporated into the final version of this document.

3. Evidence

The problem definition was based on:

- previous implementation reports and studies carried out by the Commission[114]
- the dedicated action under the Operational Action Plans 2014, 2015 and 2016 of the EMPACT sub-priority "Payment Card Fraud" of the EU Policy Cycle[115]
- the information gathered in the framework of the 7th cycle of mutual evaluation,[116] dedicated to the practical implementation and operation of the European polices on preventing and combating cybercrime.

The information available has been complemented by additional research.

This was used to update and substantiate the problems identified in those implementation reports and studies, identify possible solutions and assess their impacts (see external expertise below).

4. External expertise

As indicated above, the impact assessment work was based on previous reports and studies and partly informed by external expertise.

Following discussions with the ISG, a request for services for the impact assessment and evaluation support study was launched in August 2016 and the study was delivered in June 2017. Its draft final report including the assessment of all major impacts was scrutinised by the ISG and commented by various services of the Commission. The study relied on:

- the reconstruction of the Framework Decision intervention logic showing the objectives of the intervention and the chain of expected effects (outputs, outcomes and impacts);
- desk research on EU and national documents;
- field research, including interviews, a web based survey targeted to representatives of: law enforcement authorities in the area

[114] Two complementary Implementation Reports have been produced in 2004 and 2006: COM(2004) 346 final and COM(2006) 65 final. Moreover, relevant national provisions on non-cash payment fraud had recently been analysed under a Commission Study on criminal sanction legislation and practice in representative Member, available at http://ec.europa.eu/justice/criminal/document/files/sanctions_delivery_en.pdf, p178-232

[115] The policy cycle is a methodology adopted in 2010 by the European Union to address the most important criminal threats affecting the EU. Each cycle lasts four years and optimises coordination and cooperation on chosen crime priorities. More information is available at http://www.consilium.europa.eu/en/documents-publications/publications/2015/eu-policy-cycle-tackle-organized-crime/

[116] http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-general-matters-including-evaluation/

of data protection, victims' assistance and the private sector, and a validation focus group. Overall, 125 stakeholders have been involved in the study covering all Member States except CY, HU and HR. Moreover, the study used the results of the open public consultation that the European Commission (EC) launched in March 2017 to collect opinions on the effectiveness of the current legislative and policy framework and on existing problems and possible options for future initiatives.

The responses of the stakeholders that had only partially answered to the survey have been taken into account only when the stakeholders had provided at least one detailed response to an open question.

The survey included both closed and open questions. The analysis mainly focused on closed questions and used qualitative inputs provided by respondents to the open questions to further illustrate the results. Overall, stakeholders' inputs to open questions were generic and heterogeneous therefore making it difficult any comparison of the answers.

All questions having at least 40% of responses have been analysed. Questions with more than 60% of "No Answers entered" and "do not know" were not taken into account. Share of survey respondents indicated in the analysis have been calculated based on the total number of stakeholders who provided an answer different from "do not know" and "No Answers entered".

The analysis of the survey is structured around evaluation questions mirroring the structure of the core text. Survey questions have thus been grouped according to the main evaluation question they refer to.

The results of the consultation are presented in detail in annex 2.

www.parlament.gv.at

ANNEX 2: STAKEHOLDER CONSULTATION

Three types of consultation activities were carried out: open public consultation, targeted consultation organized by the European Commission and targeted consultation organized by a contractor:

1. Open public consultation

The European Commission launched an open public consultation on 1 March 2017, which aimed to gather feedback from the public at large on the problem definition, the relevance and effectiveness of the current legal framework in the field of non-cash payment fraud, as well as options, and their possible impacts to tackle existing issues. The consultation closed after 12 weeks, on 24 May 2017.

The open public consultation was conducted through an online questionnaire published on the internet in all EU official languages and announced at the "single access point". Two separate questionnaires were prepared: one for the general public and another one for private organisations, public authorities, or practitioners in the area of non-cash payment fraud. It was advertised on the European Commission's website,[117] through social media channels (DG HOME and Europol's EC3 Twitter accounts), through established networks of stakeholders (e.g. contacts held by the European Cybercrime Centre at Europol) and at all relevant meetings (as listed below).

Thirty-three practitioners and twenty-one members of the general public answered the questionnaires of the open public consultation. Four practitioners provided additional inputs through written contributions. Practitioners included:

- private companies (private sector);
- international or national public authorities (law enforcement agencies, judicial authorities and EU institutions and bodies);
- trade, business or professional associations (e.g. national banking federations) ;
- non-governmental organisations, platforms or networks;
- professional consultancies, law firms, self-employed consultants;

Members of the general public contributed from nine Member States (AT, BE, DE, EL, ES, FR, IT, PT, SE). Practitioners did not always specify their country of origin or residence but at least 13 Member States (CZ, DE, DK, EL, ES, FI, HU, IE, IT, NL, PT, RO, SK) were covered. Some stakeholders operated at EU level.

Results of the public consultation are analysed and integrated in this annex.

[117] See DG HOME website

www.parlament.gv.at

2. Targeted consultation organized by the European Commission

1. Large expert meetings:
    - Representatives from police and judicial authorities from all EU countries (selected by Member States) were invited to take part in two expert meetings:
        - on 2-3 May 2017, the first meeting was used to verify, validate and integrate the preliminary analysis conducted on the evaluation of the existing issues
        - on 1-2 June 2017, the second meeting was used to gather experts' views about the possible solutions to the identified problems.
    - Experts from private sector (financial institutions, payment service providers, merchants, card schemes) were invited on 31 May – 1 June to discuss the preliminary analysis conducted on the evaluation of the existing issues and present their views on priorities for action and possible solutions.

    On 1 June 2017, experts from law enforcement authorities and private sector met together to discuss challenges related to public-private cooperation.

2. Other meetings with the following experts and stakeholders:
    - Experts from academia, law enforcement agencies and virtual currencies industries, organized in cooperation with Europol (EC3) (June 2016)[118].
    - Representatives of police and law enforcement were consulted in the framework of the dedicated EMPACT Payment Card Fraud sub-priority, three times in 2016 and once in 2017.
    - Representatives of consumers' organisations were consulted in the framework of a dedicated meeting with the European Commission (16 March 2017)
    - Representatives of private financial institutions:
        - Meetings (three) of the Advisory Group on Financial Services of the European Cybercrime Centre at Europol
        - European Payment Council Card Fraud Prevention Forum (29 March 2017)
        - European Card Payments Association - Security Working Group (24 May 2017)
    - Representatives of virtual currencies industries: meeting of the Blockchain and Virtual Currencies Working Group (10 January 2017)
    - Representatives of financial regulators: the work towards a possible new initiative was discussed twice at the SecuRe Pay Forum (November 2016 and April 2017).[119]
    - Representatives from academia: Conference "Payment Card Fraud Trends – Legal Aspects" - Thessaloniki, 22 November 2016

[118] JRC Technical Report ref. JRC105233, limited distribution
[119] https://www.ecb.europa.eu/paym/pol/forum/html/index.en.html

b) A set of targeted consultations performed by an external contractor team to support the different steps of the project.

3. Targeted consultation organized by a contractor

A contractor organized targeted consultations that included online surveys and interviews. The preliminary results of the consultation were presented to a Validation Focus Group which then provided feedback as well as verified the results of the consultation.

The **survey** aimed at gathering qualitative and quantitative evidence on non-cash payment fraud (including counterfeiting) in order to assess the dimension of crime and understand the positions and perspectives of the different stakeholders acting at national and at EU level. The survey mainly included a set of predefined questions with some open-ended questions to allow participants to contribute with more detailed opinions or advice. The survey was targeted to representatives from law enforcement and judiciary, data protection authorities, national banking federations, associations and civil society organisations as well as other stakeholders from the private sector.

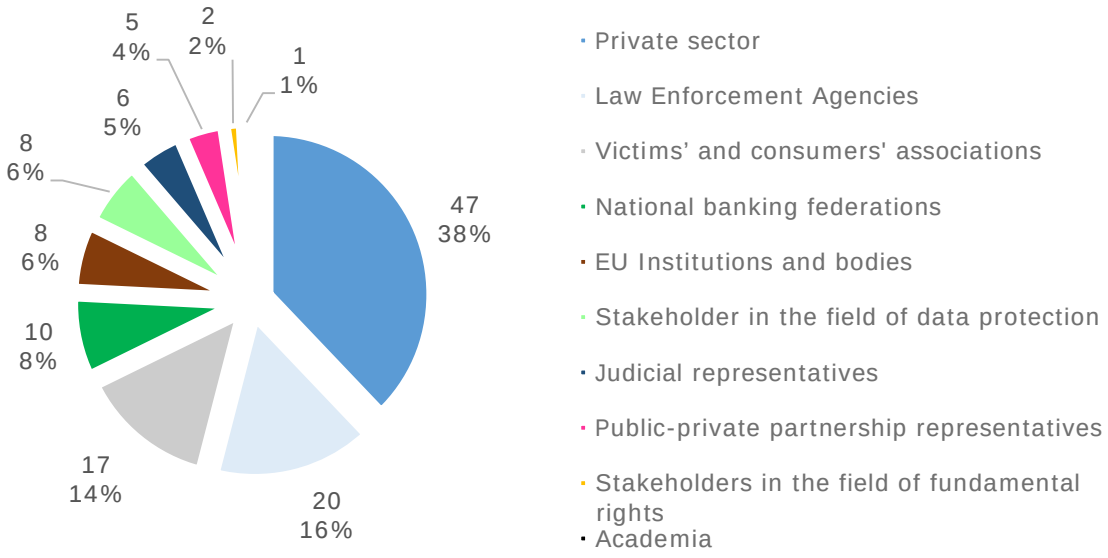
The purpose of the interviews was to complement the information collected through the surveys by filling in the possible data gaps and by improving the understanding of the responses. In particular, interviews allowed to: (i) gather information related to the implementation of the EU framework by pointing at loopholes and specific issues deserving further attention; (ii) deepen the understanding of the recent technological developments and future trends in non-cash payment fraud in order to design up-to-date and realistic policy options; (iii) support the identification of relevant cases of public-private cooperation and (iv) gather recommendations and suggestions in order to improve the prevention and fight against non-cash payment fraud.

An online **Validation Focus Group** was organised on 11 April, 2017 with the aim of presenting the main findings of the evaluation study, illustrating expected policy options and gathering input on their impacts.

Overall, 125 stakeholders[120] were involved covering all Member States except CY, HU and HR. The figure below illustrates a detailed category breakdown of the stakeholders. All categories initially identified have been involved.

[120] Some stakeholders have been targeted through several data collection tools.

Figure 1: stakeholders consulted through targeted consultations



When looking at stakeholders addressed through the different data collection tools, the evaluation team collected answers to the **survey** from 88 stakeholders including 21 representatives from law enforcement authorities, 19 representatives from associations and data protection authorities, 10 representatives from national banking federations and 38 representatives from the private sector.

53 stakeholders were **interviewed** including 11 representatives from law enforcement, 6 from the judiciary, 10 from associations and data protection authorities, 5 representing public-private partnership, 1 from Academia, 1 from legal practitioners, 2 from national banking federations, 9 from the private sector and 8 from EU institutions and bodies.

7 stakeholders attended the **Validation Focus Group** including representatives from EU institutions and bodies, the private sector, public-private partnership, law enforcement and Academia.

Main results

Dimension of crime

Costs related to non-cash payment fraud were generally perceived as high and were expected to increase in the coming years. Stakeholders from all categories faced difficulties when asked to quantify the criminal phenomenon. Statistics are rare[121] and not always accessible. Some of them[122], however, provided case-based evidence implying the significance of certain types of non-cash payment fraud.

[121] Interview feedback: one representative from victims association and three from the private sector.
[122] Interview feedback: six representatives from LEA, two from the public-private partnerships, one from the victims associations and academia and one from EU institution and bodies.

www.parlament.gv.at

Stakeholders from national banking federations reported an increase of transactions that resulted in consumers' complaints following the misuse of a non-cash payment. This trend could be seen since the 1990s. Some private sector representatives indicated that that this trend was decreasing. As regards to investigations, prosecutions and convictions related to non-cash payment fraud, it is not clear whether they have increased after the entry in force of the Framework Decision.[123]

Payment instruments have evolved over the years with the introduction of an increasing number of non-corporeal payment instruments, such as virtual currencies, e-money and mobile money. Techniques to commit non-cash payment fraud have evolved and they have become increasingly sophisticated. Stakeholders from different categories[124] acknowledged the increasing importance of new forms of cyber-related crime, mainly relating to card-not-present fraud, social engineering and virtual currencies, and suggested further improvement both in terms of protection and in terms of comprehensive definitions (e.g. offences linked to phishing and carding)[125]. Data breaches, malware and phishing are considered the most important means to obtain credentials to be used in fraudulent transactions (with private enterprises showing the highest level of concern). [126] There is a general consensus that several actors bear the costs of non-cash payment fraud, namely banks, financial institutions, merchants and customers.[127]

Identity theft is reported to be an emerging concern. No statistics have been provided by stakeholders. However, there is an overall concern about the relevance of the phenomenon, its expected evolution, and the limited level of protection ensured by the current legislative framework.[128] The vast majority of stakeholders agree that identity theft should be criminalised.[129] As a further confirmation of the increasing importance of identity theft, most representatives from the law enforcement confirmed that carding websites are investigated in their countries.

Criminal law framework

Most stakeholders consulted consider the current EU legal framework only partially relevant to security needs, especially concerning the definition of payment instruments and criminal offences. Some confirmed that national frameworks would need to be amended.

[123] Survey feedback: 37 representatives from law enforcement authorities, 8 from Associations and data protection authorities and interview feedback of 13 representatives of law enforcement authorities and 2 from Judicial coop. rep.
[124] Survey feedback from private sector, national banking federations, stakeholders in the area of data protection, law enforcement authorities and interview feedback from four representatives from law enforcement authorities, one from Judicial coop. rep., two from PPP, one from legal practitioners, one from banking fed., two from private sector, one from victims associations and academia and one from EU Institutions and bodies
[125] First Expert Group Meeting (Public Sector)
[126] Open public consultation feedback: international or national public authority, private enterprises, Professional consultancy, law firm, self-employed consultant, Trade, business or professional association and other categories
[127] Survey feedback: twenty representatives from law enforcement authorities, eight from national banking federations and thirty-five from the private sector
[128] Stakeholders from the First Expert Group Meeting (Public Sector) pointed out that in Estonia identity theft is punishable independently from fraud-related provisions, but require some kind of damage (moral or other)
[129] Open public consultation feedback: 85% (n=18) of the stakeholders form the general public

The Framework Decision is considered by the private sector, law enforcement authorities, associations and data protection authorities and national banking federations to be only partially relevant to current security needs, especially with regard to the definition of payment instruments and criminal offences.

As for the definition of payment instrument, the Framework Decision is considered to be not appropriate in so far as it does not cover all newer forms of electronic payments such as online banking payments, mobile payments, electronic wallets, bitcoins, and more generally internet payments. It covers means of payment that no longer exist and it is not consistent with the definition of 'payment instrument' included in the Payment Services Directive which goes beyond 'corporeal' instruments.

As for the forms of conduct that can be sanctioned in relation to non-cash payment fraud, there is a strong consensus among all categories of stakeholders that the Framework Decision is not comprehensive, and that there are emerging trends that should be better covered. These relate mainly to online fraud and more specifically to theft of credit card credentials, phishing[130] and fraud related to the use of virtual currencies. Activities such as acquisition[131] and sale[132] of credentials to be used in fraudulent transactions should be criminalised according to almost all of the stakeholders, together with fraudulent transactions with virtual currencies[133] and online transactions with stolen credentials.[134]

National penalties established for the offences covered by the Framework Decision are perceived to be somewhat effective in tackling non-cash payment fraud. Private sector representatives together with representatives from the public-private partnership were most dissatisfied. Poor enforcement of penalties seems to be among the reasons for their limited satisfaction. Also, most of the stakeholders[135] agreed that it is necessary to have a more coherent level of penalties for offences related to non-cash means of payment across the EU. The Anti-Money Laundering Directive and investigations related to it have been mentioned by stakeholders from the public sector as examples to be looked at in order to determine sanctions and penalties. Also the need to look for aggravating circumstances for organised crime has been highlighted.[136]

In general, there is poor knowledge of the Framework Decision among stakeholders from the private sector and law enforcement authorities. They found it difficult to identify the contribution of the Framework Decision to their national legislative frameworks, and to the evolution of the criminal phenomenon. Too many years has passed since its adoption. Other

[130] First Expert Group Meeting (Public Sector)
[131] Open public consultation feedback: 90% (n=19) of the stakeholders form the general public
[132] Open public consultation feedback: 95% (n=20) of the stakeholders form the general public
[133] Open public consultation feedback: 95% (n=20) of the stakeholders form the general public agreed to different extent, only one representative totally disagreed
[134] Open public consultation feedback: nearly 100% of the stakeholders form the general public
[135] Open public consultation feedback: thirty-two representatives from private sector, eleven from trade, business or professional association, one from professional consultancy, law firm, self-employed consultant, two from non-governmental organisation, platform or network
[136] First Expert Group Meeting (Public Sector)

www.parlament.gv.at

EU and international instruments have complemented the Framework Decision and partially overlap with its scope.

Procedural criminal law

Stakeholders consider the current level of cooperation between Member States for investigations and prosecutions as needing improvement.

With regard to investigations, obstacles relate mainly restrictions hampering information sharing among competent authorities: lengthy procedures, the need to collate different sources of information to have the whole picture[137]. There are also disparities between policies applied by different actors[138]. Moreover, there is a limited possibility for some law enforcement authorities (mainly due to the principle of legality) to prioritise and select non-cash payment cases to be followed up with investigations and internal resources are insufficient to analyse the information provided by the private sector.[139] These elements make non-cash payment cases a low priority in the agenda of some Member States, and therefore limit the effectiveness of investigations. This applies particularly to cross-border cases (further affected by a lack of universal communication channels). Europol also highlighted the anonymity of data exchange and financial transactions as a challenge to law enforcement.

Europol's support in facilitating cross-border cooperation is widely acknowledged. In addition, stakeholders also appreciates European platforms for data sharing such as SIENA and the need arose for a secure system for cross-border sharing of information among stakeholders affected by non-cash payment fraud. Europol stressed the importance of a harmonised legal framework including penal laws and sanctions as well as procedural laws.

Some experts from the public sector[140] indicated Joint Investigations Teams as an effective way to cooperate and exchange information, while other experts stressed difficulties and administrative formalities in setting them up.

Some respondents from associations and data protection authorities consider that there are obstacles in prosecutions. Obstacles for investigations may also affect prosecutions. In particular, several stakeholders stressed that timely cooperation remains an issue, since – when involving different legislation – it may take time to gather the needed information and evidence for prosecutions.

The majority of stakeholders felt that the current rules of jurisdiction allow for effective investigation and prosecution of crime. However, some respondents from the private sector perceive that the issues connected with the international/cross-border dimension of non-cash payment fraud do not allow effective investigation and prosecution of crime. Stakeholders reported case-based evidence on criminal activities that could not be investigated or prosecuted because of jurisdictional issues and, where present, reasons relate more to

[137] First Expert Group Meeting (Public Sector)
[138] First Expert Group Meeting (Public Sector)
[139] First Expert Group Meeting (Public Sector)
[140] First Expert Group Meeting (Public Sector)

www.parlament.gv.at

operational obstacles rather than legal loopholes. Examples of obstacles encountered when involving different jurisdiction include, for instance, cooperation between private entities and victims of a crime with foreign authorities.[141]

In this context, stakeholders acknowledged the relevance of the support offered by Eurojust to solve cross-border jurisdictional issues.

Reporting to law enforcement authorities

Views on reporting to law enforcement authorities differed: some were satisfied with the current level of reporting, while others believed it should be improved. Under-reporting might be due to reputational concerns of private sector representatives when victims of non-cash payment fraud[142].

The different categories of stakeholders agreed that future policy options on reporting need to be balanced with the actual capacities of law enforcement authorities to follow-up on cases. Europol pointed out that compulsory reporting will likely cause problems and voluntary reporting in a structured manner would be preferable while other public sector experts conveyed that reporting should be mandatory.

Public-Private Cooperation

Stakeholders felt that cooperation between public and private entities was beneficial overall and agreed that it should be encouraged to better tackle non-cash payment fraud, particularly when it comes to prevention[143].

Most of the stakeholders considered that public-private cooperation should be improved to combat non-cash payment fraud. Private sector representatives appeared to be the most dissatisfied. They perceive the main obstacles to cooperation to include, for instance, limitations in the possibility to share information with law enforcement authorities and in related tools used to enable the exchange.

The vast majority of stakeholders[144] agreed that in order to investigate and prosecute criminals, financial institutions should be allowed to spontaneously share with the national police or the police of another EU country some of the victim's personal information (e.g. name, bank account, address, etc.).

Poor cooperation among private and public authorities has also been mentioned by several stakeholders[145] as an obstacle encountered when fighting non-cash payment fraud.

[141] First Expert Group Meeting (Public Sector)
[142] First Expert Group Meeting (Public Sector)
[143] First Expert Group Meeting (Public Sector)
[144] Open public consultation feedback: general public
[145] Open public consultation feedback from international or national public authority, private enterprises, Professional consultancy, law firm, self-employed consultant, Trade, business or professional association and other categories

www.parlament.gv.at

Legislation, misalignment of priorities and lack of trust together with practical and organisational issues are seen as obstacles by private enterprises, public authorities, trade, business or professional associations for a successful cooperation between public authorities and private entities when actors are based in different EU countries.[146]

Stakeholders from law enforcement authorities and from the private sector suggested that cooperation among Member States can be developed through both formal and informal partnerships. Successful cooperation initiatives include for instance initiatives promoted by Europol (such as the e-Commerce Working Group in 2014 and the Memorandum of Understanding between Europol-EC3 and European Bank Federation), the Italian platform OF2CEN (and the related EU project EUOF2CEN), the British DCPCU, the French GIE Carte Bancaire, a working group in Slovakia gathering national financial institution and a EL sectorial cooperation to combat fraudulent purchase of plane tickets. An increased sharing of good practices and successful cooperation initiatives is generally welcomed by private sector representatives.

Victims' rights

Damage for victims resulting from non-cash payment fraud is perceived as including violations of the right to the protection of personal data, financial losses and theft of credentials, while stakeholders give a lower degree of importance to the impact of non-cash payment fraud on the willingness to make transactions online and the access to online services.

Stakeholders stressed the importance of protecting victims of fraud. Some of them felt that victims are not protected sufficiently. National initiatives aiming at enhancing protection are overall appreciated[147]. Victims associations have developed good cooperation mechanisms with law enforcement authorities. They aim at providing concrete assistance and encourage victims to report crimes. Countries like UK and NL have developed national helpdesks (online tools at disposal of victims of fraud) which assist victims and provide prevention materials.

The protection of victims as regards identity theft is considered an area where further improvement is needed and several representatives from associations and data protection authorities considered the level of protection of victims' rights in these cases to be only partially effective. Overall, identity theft is perceived as affecting natural persons as well as legal persons. Therefore victims should be protected regardless of their legal statute.

[146] Open public consultation feedback from international or national public authority, private enterprises, Professional consultancy, law firm, self-employed consultant, Trade, business or professional association and other categories

[147] Some experts from the First Expert Group Meeting (Public Sector) called for keeping issues regarding consumers' protection (such as the negative impact on the credit history of a non-cash payment victim) separate from criminal law.

www.parlament.gv.at

Victims are also perceived to be in need for psychological support and support to recover losses, getting information on different forms of crime related to non-cash means of payments and the possibility for consumers to prove the occurrence of an unauthorised transaction.

In this regard, representatives from associations and data protection authorities, private sector and national banking federations mentioned some examples of good practices including, for instance, dedicated websites, educational and awareness campaigns as well as brochures and guidelines.

Other results

The effects on SMEs have been described in the qualitative assessment part of the report, both in section (5.1) and in annex 4.

In terms of minority views, the most relevant cases of minority/dissenting views have been described in the relevant sections of the report. These include:

- The dissenting views concerning the deterrence effect and the general effectiveness of a common minimum level of maximum penalties (section 1.3.1. on problem drivers);
- The different views concerning the creation of an EU database on fraud data.
  Some stakeholders from the private sector raised this possibility during the expert meetings, but others questioned its viability (see section 4.2.2 on policy measures discarded).

Synthesis of the contributions provided in the open public consultation

1. Contribution from a law enforcement agency:
   A national law enforcement agency supports the adoption of a new legal framework for facilitating investigations of non-cash payment fraud, which would make the procedures in obtaining evidence from other countries less time-consuming. The main problem identified is that investigating authorities do not receive timely responses and information exchange between the affected countries should be improved.

2. Contribution from a consumers' association:
   A consumers' association points out possible shortcomings in the implementation of the revised Payment Services Directive, which introduces too many derogations to strong customer authentication requirements.

3. Contribution from a national banking federation:
   A national banking federation calls for a more harmonised framework for fighting non-cash payment fraud as fraudsters and organized crime groups target consumers and banks without regard to borders. They also highlight the fact that victims of so called "push payment" fraud, or common fraud scams and swindles, have little or no recourse for reimbursement.

www.parlament.gv.at

With current means, law enforcement authorities face considerable workload due to the long time needed to complete the fraud trail, in order to initiate investigation, attribution, possible arrest and prosecution.

This banking federation calls for facilitated exchanges of information and intelligence between banks, national law enforcement agencies and Europol at both national and EU level in order to enable the tracing and freezing of stolen assets.

The existing current data protection law is perceived as constraining information exchange and hampering the ability to detect financial fraud compared with other EU member states.

They support the revision the Framework Decision and wish that the revised legislation contains clearer guidance regarding the sharing of information and intelligence.

4. Contribution from a private company providing and distributing prepaid services
This private company clarifies that prepaid means of payment cover the following instruments:

   - social vouchers (corporeal and non-corporeal), which allow to dedicate funds to a specific usage in one Member State, as determined by a social framework;
   - anonymous prepaid cards, which permit anonymous transactions but with a restricted framework. They can be of different types depending on whether they allow for an access to cash, have product limits and can be used outside the Member State territory.

This company highlights that prepaid e-money cards are covered by the PSD2 and so are then subject to rules of strong authentication. However, social vouchers and limited prepaid instruments are excluded from the scope of the PSD2 but their characteristics extremely limit possible fraudulent usages.

Thus, they believe that the use of prepaid instruments, and in particular social vouchers and limited prepaid instruments, present insignificant risk of fraudulent use and of counterfeiting.

ANNEX 3: WHO IS AFFECTED BY THE INITIATIVE AND HOW

Who is affected	How is affected
Payers	The initiative would not impose (directly or indirectly) new obligations on payers. In general, the objective of diminishing the risk for consumers of being victims of fraud and the associated financial losses would have a positive impact on consumers' trust in non-cash payment transactions. This is particularly true for those using newer means of payment, for which the initiative would step up protection, through the adoption of a technology neutral definition. Possible provisions on reporting and prevention would not entail obligations for payers. Possible considerations of consequences of fraud as aggravating circumstances (e.g. identity theft) would improve protection for victims. By diminishing fraud, the initiative would possibly have a positive impact on charges for payers, on the medium term.
Enablers	The initiative would not impose (directly or indirectly) new obligations on enablers. By diminishing fraud, the initiative would possibly have a positive impact on costs for enablers, on the medium term, by reducing the cost of doing business. By adopting a technology neutral definition, the initiative would contribute at ensuring that enablers are all equally protected, therefore favouring competition. The initiative would aim at improving the level of cooperation between public institutions and private sector and facilitating the establishment of Public-Private Partnerships. On the one hand, stronger public-private cooperation would enable the exchange of strategic information which could improve prevention, reduce the risk of being victim of fraud and improve consumer choice; on the other hand, as provisions on reporting will not by compulsory, economic operators would be allowed to report relevant incidents (that are likely to lead to significant financial losses to them if not contrasted) while not bearing additional costs due to mandatory reporting.
Payees	The initiative would not impose (directly or indirectly) new obligations on payees. By diminishing fraud (and contributing to target especially cross-border fraud), the initiative would possibly have a positive impact on costs for payees, on the medium term, by reducing the cost of doing business, increasing consumption and trade flow and saving costs related to fraud preventions. The initiative would aim at improving the level of cooperation between public institutions and private sector and facilitating the establishment of Public-Private Partnerships. This would enable the exchange of strategic information which could improve prevention, reduce the risk of being victim of fraud and improve consumer choice, while allowing economic

www.parlament.gv.at

	operators to report relevant incidents (that are likely to lead to significant financial losses to them if not contrasted) without bearing additional costs due to mandatory reporting.
Law enforcement, judicial authorities, Member States, EU	Law enforcement and judicial authorities would face the greatest burden as a consequence of the initiative: a broader definition of means of payment and additional offences to be tackled (preparatory acts) is likely to increase the number cases that police and judicial authorities are responsible for. On the other hand, the establishment of a clear legal framework to tackle enablers for non-cash payment fraud, such as the sale of stolen credentials, would provide a chance for detecting, prosecuting and sanctioning fraud-related activities earlier on, while still in the phase of preparation. Additional resources would be required to step up cross-border cooperation and the capacity of points of contact. Equally, an obligation for Member States to gather statistics would create a certain administrative burden, in terms of possibly adapting systems in place for law enforcement to record cases and in terms of elaborating those statistics at national level, before transmitting them to Eurostat. By enhancing public-private cooperation, the initiative aims at creating the conditions for law enforcement authorities to be more effective, by more easily establishing the links between cases and tackle non-cash payment fraud in a strategic manner. While public-private cooperation has a cost in terms of resources, the return on investment in terms of effectiveness and efficiency of law enforcement action is immediate. Overall, the cumulative impact of these measures on administrative and financial costs could be higher than in baseline, as the numbers of cases to be investigated would put strain on law enforcement resources in this area, which would need to be increased.

Summary of costs and benefits for the preferred option

The tables below summarize the costs and benefits for the preferred option. Given the limitations in the impact assessment created by the lack of available data, the tables have been filled to the extent possible:

Costs:

I. Overview of costs – Preferred option (million EUR)							
Policy measure		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
3	Direct costs					0.070	0.527
	Indirect costs						
5	Direct costs					0.210	0.689
	Indirect costs						
7	Direct costs					0.070	0.045
	Indirect costs						
11	Direct costs					0.070	0.702
	Indirect costs						
12	Direct costs					0.070	0.253
	Indirect costs						
14	Direct costs					0.070	0.070
	Indirect costs						
Total preferred option	Direct costs					**0.561**	**2.285**
	Indirect costs						

As discussed in section 5.2. (quantitative assessment), the costs for national administrations (direct) include:

- One-off costs:
  - Transposing EU legislation in Member States.
- Continuous costs:
  - Implementing and enforcing the new legislation, in particular when it leads to an increase in the number of cases to be investigated.
  - Facilitating cross-border cooperation, including collection of statistics, operation of contact points (also for reporting purposes) and cooperation with Europol and Eurojust.
  - Implementation of awareness raising campaigns.

No costs were identified for citizens/consumers and businesses.

Benefits:

II. Overview of Benefits (total for all provisions) – Preferred Option (million EUR)		
Description	***Amount***	***Comments***
Direct benefits		
Reduction of fraud	144	Payers, payees and enablers would directly benefit from the reduction of fraud
Indirect benefits		

As explained in section 5.2. (quantitative assessment), given the limitations caused by the lack of data, the calculation of benefits was carried for the main purpose of comparing the options. Therefore, the total value of benefits must be interpreted in relation to the other options, rather than as an accurate estimate of the actual reduction of fraud that the preferred policy option would actually cause.

REFIT potential

REFIT Cost Savings – Preferred Option(s)		
Description	***Amount***	***Comments***

With regard to the REFIT potential of the preferred option, it can only be assessed from a qualitative point of view, as explained in section 5.3. (REFIT potential).

www.parlament.gv.at

ANNEX 4: ANALYTICAL MODELS USED IN PREPARING THE IMPACT ASSESSMENT

A4.1. Qualitative assessment

A4.1.1. Qualitative assessment of the policy measures

The qualitative assessment of the retained **policy measures** (including which stakeholders are mostly concerned by each measure) is the following:

0 : Baseline			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	Maintaining the baseline is unlikely to address neither of the two general objectives.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	Maintaining the baseline is unlikely to raise specific issues since the Framework Decision is already coherent with the main EU legislation dealing with non-cash payment fraud. At the same time, neither additional synergies nor mutual reinforcing effects can be expected.

www.parlament.gv.at

0 : Baseline			
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	The level of law enforcement capacity to address non-cash payment fraud is related to the level of reporting required by the current legislation (although it is also affected by other factors, such as prioritisation compared to other issues that LEAs have to address). The evaluation showed that there are no specific provisions on reporting of non-cash payment fraud incidents to LEAs and thus there is no consistent framework on reporting activities among Member States. This somewhat hampers their capacity to deal with fraud cases with an international dimension. There are also no standards to outline appropriate actions to report data breaches and internet crimes to LEAs making it difficult to identify the source of such breaches and the consequent detection of illegal transactions. In the baseline scenario (i.e. with no further EU action) the responsibilities and capacity of LEAs in this respect could remain largely the same. With an increased number of fraudulent transactions, and assuming the same level of resources available to LEAs, their capacity to address criminal activity may be negatively affected.
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	The evaluation exposed a number of barriers to detecting, prosecuting and sanctioning non-cash payment fraud criminals (e.g. inadequate provisions and discrepancies in addressing new types of payment instruments, new forms of fraud, lack of uniform know-how and insufficient expertise of LEAs and judicial authorities and the level of cooperation between Member States in international fraud cases; discrepancies in provisions establishing competent jurisdiction and in rules on extradition). In the baseline scenario (i.e. with no further EU action) the chances of detecting, prosecuting and sanctioning criminals could remain largely the same. With an increased number of fraudulent transactions, and assuming the same level of resources available to LEA and the judiciary, their capacity to pursue (prosecute and sanction) criminals may be

www.parlament.gv.at

0 : Baseline			
			negatively affected.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	The Framework Decision does not include provisions ensuring a minimum level of penalties and sanctions that could potentially discourage fraudsters and prevent a number of criminal acts. This suggests that with no further EU action the trend of increasing (card) fraud is likely to continue because payment card fraud is still considered low risk and highly profitable criminal activity: it is estimated that fraudulent activities bring organised crime groups around 1.5 billion Euro per year. In the baseline scenario these gains are likely to continue and their impact on the society could be moderate. The stakeholders mostly affected by this situation are private sectors representatives and individual customers.
		► Increasing protection for victims of non-cash payment fraud;	Victims of non-cash payment fraud suffer the costs of defending their rights, distress and other negative consequences such as negative credit ratings. The Framework Decision does not include provisions ensuring a minimum level of protection both in terms of specific rights (granted to the natural and legal persons that are victims of non-cash payment fraud). The evaluation showed that the level of protection of victims differs between Member States and that victims do not have sufficient information on the reporting systems in place and have limited knowledge of the victims' protection (different from one Member States to another). So far no provisions address explicitly the victims of identity theft. With no further EU action in this area the level of protection for victims of non-cash payment fraud is likely to remain the same.

www.parlament.gv.at

0 : Baseline			
		► Stronger cooperation between public institutions/private sector.	While the Framework Decision does not directly address public-private cooperation in non-cash payment fraud, the evaluation identified several forms of partnerships established to fight cybercrime more generally (with few public-private partnerships aimed to address exclusively non-cash payment fraud). However, it is not clear if there are successful examples of such cooperation in all 28 Member States. With no further EU action the level of cooperation between public institutions and private sector is likely to remain the same.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	The evaluation showed that there is a steady increase in number and value of non-cash payment transactions which is likely to continue in the baseline scenario (i.e. without additional EU action) (an average 5% increase in value over last 7 years). This increase is driven by a number of factors. With the baseline these factors could remain in place and continue to affect the number and value of non-cash payment transactions.

www.parlament.gv.at

0 : Baseline			
		► Increasing consumer choice due to reduction of fraud	The evaluation showed that there is an increase in the value of fraudulent card transactions. The fastest growth is observed for CNP (card not present) share in the total value of fraud. In the baseline scenario consumers are likely to be increasingly exposed to fraud and related financial losses or negative credit ratings. Fraud is likely to affect more consumers, as more people will use cards and non-cash payment transactions more generally. People who are concerned about the risk of fraud in non-cash payment transactions may avoid new or unknown firms and this may reduce competition and to some extent their choice. Consumers suffer the consequences of fraud, including financial losses and consequences derived from identity theft.

www.parlament.gv.at

0 : Baseline			
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	The evaluation showed that the vulnerability of financial institutions and commerce to non-cash payment fraud increased overall. The cost of protection for financial institutions also went up due to new forms of crime that directly affect the non-cash payment landscape, from different malware to phishing, pharming, hacking, social engineering and more. So the mobile payments firms invest more in fraud protection to ensure their net profits and limit possible excessive financial losses due to fraud crimes. Furthermore, the evaluation showed that current EU provisions do not ensure a minimum level of protection in terms of specific rights (granted to the natural and legal persons that are victims of non-cash payment fraud) and as a result, significant differences in this area exist between Member States. There are also no provisions addressing explicitly the primary and secondary victims of identity theft. In the baseline scenario (i.e. with no further EU action), these shortcomings and differences will continue. The costs of increased fraudulent transactions will be borne mainly by private sector representatives (retail sector and financial service industry). There is no data indicating how SMEs are affected by fraud it is not possible to indicate whether this group is more (or less) exposed to fraud risks. However, given SMEs form a large proportion of economic operators in the EU, this negative impact could affect many of them.
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	With no EU action in this area the administration burden could be largely unchanged.
	Simplification benefits		The baseline will have no impact on simplification benefits.

www.parlament.gv.at

0 : Baseline		
Fundamental rights	► Personal data protection;	The Framework Decision does not explicitly refer to personal data protection, with no direct obligations for Member States in this regard. Personal data continues to be stolen and used for fraudulent non-cash payment transactions. This is likely to continue without EU action and bear economic and social costs (economic losses, costs of defending their rights, distress, negative credit ratings) explained above. With the baseline scenario, the perception of security will remain largely the same.
	► Right to liberty and security	In the baseline, non-cash payment fraud would continue to be a source of income for organized crime, which has a negative impact on the right to liberty and security.
	► Freedom to conduct business;	In the baseline, new business opportunities relying on new payment instruments not covered by the current legal framework could continue to be hampered, with a possible negative impact on the freedom to conduct business.
	► Consumer protection	As noted above, there are no provisions in the Framework Decision ensuring a minimum level of protection for victims of non-cash payment fraud and a minimum level of penalties and sanctions for fraud criminals. As a result, there are differences in national legislations regarding such provisions. With no further EU action the level of consumer protection is likely to remain the same.
	► Right to an effective remedy, in particular the remedies available before the courts.	No significant impact.
EU added value		The baseline would have no impact on EU added value.

www.parlament.gv.at

1: Improve implementation			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	Improving implementation and enforcement is unlikely to have a major impact on the general objectives.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD2:** PSD 2 states in its preamble that the cooperation between the national competent authorities responsible for granting authorisations to payment institutions, carrying out controls and deciding on the withdrawal of any authorisations granted, has proven to work satisfactorily. In parallel, it is mentioned that the cooperation between competent authorities should be enhanced, both with regard to the information exchanged as well as a coherent application and interpretation of this Directive, where an authorized payment institution would like to provide payment services in another Member States by "passporting", including through the internet. Overall there is a need for enhancing the cooperation between competent authorities on information exchange and a need for guidance for the interpretation of PSD2 in respect to passporting services, including through the internet. **Directive on Attacks against information systems:** The Directive aims to establish minimum rules concerning the definition of criminal offences in respect to the attacks on information systems. It promotes the improvement of cooperation between competent authorities (police and other

www.parlament.gv.at

1: Improve implementation			
			specialised law enforcement), as well as the competent specialised EU agencies and bodies (Eurojust, Europol, European Cyber Crime Centre and ENISA). Moreover, the Directive promotes the efforts to provide adequate training to the relevant authorities on cybercrime and its impact, and to foster the cooperation and the exchange of best practices at EU level. According to Art. 13, Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week in order to perform the exchange of information. Overall, the Directive promotes the improvement of cooperation between the Member States competent authorities and the need to provide adequate training to the relevant authorities on cybercrime and its impact. **Directive on Euro counterfeiting:** The Directive sets up the possibility for investigators and prosecutors of currency (notes and coins) counterfeiting offences, to make use of effective investigative tools, such as the interception of communications, covert surveillance including electronic surveillance, the monitoring of bank accounts and other financial investigations, in accordance with national law and commensurate with the nature and gravity of the offences under investigation. Overall, the Directive sets up the possibility for investigators and prosecutors of currency (notes and coins) counterfeiting offences, to make use of effective investigative tools **Regulation on interchange fees for card-based payment transactions:** Art. 13 of the Regulation states that Member States shall designate competent authorities that are empowered to ensure enforcement of the Regulation and that are granted investigation and enforcement powers. Overall, the Regulation empowers the competent authorities with investigation and enforcement powers. **NIS Directive:** The Directive maintains a high level of security of network and information

www.parlament.gv.at

1: Improve implementation			
			systems. Member States have to designate competent authorities responsible for fulfilling the tasks, as well as a single point of contact, responsible for coordinating issues related to the security of network and information systems. Member States are requested to have in place a national strategy on the security of network and information systems. Member States have the obligation to communicate their national strategies to the Commission. Each Member State has a computer security incident response team's network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation. A Cooperation Group has been created to provide the strategic guidance for the activities of the CSIRTs, exchanging best practice on the exchange of information. At EU level there is a network formed by national CSIRTs and CERT-EU. ENISA also assists and provides the expertise and advice in order to facilitate the exchange of best practice. Overall, the Directive promotes the adoption of the national security strategy and the development of the cooperation at national and international level, including through guidance. **Directive on Victims' Rights:** Art. 26 of the Directive makes reference to the coordination and cooperation between Member States in order to improve the access of victims to their rights. The Directive promotes the need for assuring the training for lawyers, prosecutors and judges and for practitioners who provide victim support or restorative justice services. Thus, the practitioners who are likely to receive complaints from victims have to be appropriately trained in order to facilitate reporting of crimes. Overall, the Directive promotes cooperation between the Member States and training of practitioners for improving the access of victims to their rights. However, this Directive only covers natural persons, not legal persons. Also, it does not include specific provisions on identity theft.

www.parlament.gv.at

1: Improve implementation			
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	This measure focuses on investing in the capacity of LEAs through training courses, additional guidance and tools, sharing best practice, information and communication campaigns. As a result of these actions, LEAs capacity could increase. However, with the legal provisions unchanged, LEAs will still be limited in their abilities to prosecute new methods of fraud or fraud activities related to non-cash means of payment. Overall, better implementation measures could show minor improvements over the baseline. The main stakeholder groups affected by this will be **LEAs, judiciary & judicial cooperation representatives**, **legal practitioners.**

www.parlament.gv.at

1: Improve implementation			
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	Training, improved cooperation and sharing best practices among **LEAs, judiciary and legal professionals** could reinforce investigations and prosecutions in the relevant areas of non-cash payment fraud (although these will still be limited to current legal provisions). The impact of this measure is still expected to be higher than the baseline. These stakeholder groups (i.e. **LEAs, judiciary and legal professions**) would be also the main ones concerned with this initiative. A higher level of detection will translate in incrementally higher workload for the justice system. However, the benefits of increasing chances of detecting, prosecuting and sanctioning criminals would also translate into gains for **individual customers** and **economic operators,** as perpetrators might be (temporarily) inhibited from fraudulent activities.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	The number of criminal acts related to new forms of non-cash payment fraud could be at a similar level as in the baseline scenario. However, with improved implementation and enforcement, organised crime gains are likely to be rising slower than in the baseline. This is because the prosecution could be reinforced. Overall, the expected magnitude of the impact is likely to be small. The stakeholders mostly affected by this change are **private sector representatives (economic operators)** and **individual customers**.
		► Increasing protection for victims of non-cash payment fraud;	Better implementation and enforcement of current provisions could effectively improve the level of protection for victims of non-cash payment fraud compared to the baseline scenario, thanks to possible improvements in detection, prosecution and sanctioning. However, this increased protection is likely to be limited, given that the scope of the legislation remains the same. The stakeholders most likely to benefit from this are **private sectors representatives (economic operators)**.
		► Stronger cooperation between public institutions/private sector.	Guidance, information and best practice examples developed by the Commission and shared among different stakeholders could improve the level of cooperation, including between public institutions and the private sector. However, the magnitude of this change is likely to be limited. The main stakeholders affected by this change are **LEAs, private sector representatives, banking federations** and **public-private partnerships**.

www.parlament.gv.at

1: Improve implementation			
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	Improved implementation and enforcement of the Framework Decision, PSD2 and e-money Directive could bring similar effects to the baseline in terms of increased consumption and trade flows measured by the number and volume of non-cash payment transactions. This is because this measure introduces training, guidelines and communication campaigns to raise awareness of non-cash payment fraud and best practices in addressing it. The impact of this measure might be a little higher compared to the baseline because these activities are likely to lead to increased level of trust and improved perception of security of non-cash payment transactions. However, the increase would still be rather moderate. The same stakeholders as in the baseline would be affected.
		► Increasing consumer choice due to reduction of fraud	Improved implementation and enforcement of current provisions, accompanied by increased capacity of LEAs through training and guidelines, could lead to reinforced investigations and prosecutions in the relevant areas of non-cash payment fraud especially around fraudulent cards and cheques. However, a large share of fraudulent activities (related to non-cash means of payment and new forms of crime) would still remain unregulated. As a result, the level of fraud could continue to grow but because some areas would be better protected, this trend could be a little slower than in the baseline. The same stakeholders as in the baseline would be affected, albeit to a smaller extent.
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	Similar to the effects on consumer choice and reduction of fraud, better implementation and enforcement of current provisions could mean minor cost savings for economic operators. However, new payment instruments would remain uncovered by the legislation. These areas would still require significant investments from economic operators to minimise the risks of fraud as they are the primary targets of non-cash payment fraud and card fraud activities in particular. As a result, the level of fraud (and the costs of protection against fraud) could continue to grow albeit slower than in the baseline The same stakeholders as in the baseline would be affected, albeit to a smaller extent. Again, while no detailed analysis of this impact on SMEs, improvements of the situation compared to the baseline would be beneficial for SMEs, as they form a large proportion of economic operators in the EU.

www.parlament.gv.at

1: Improve implementation			
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	With improved implementation and enforcement of current provisions, the administration burden could increase. This is because better implementation could lead to more fraud cases being detected & prosecuted. This in turn would require additional administrative efforts at the national level. The legal basis for prosecuting the fraud cases would remain unchanged. On the other hand, the EU institutions could be more affected. This is because this measure requires the following investments: - one-off costs for the EU: publication of the 3rd implementation report of the Framework Decision; publication of a guidebook on national legislation to foster cooperation - continuous costs for EU: training courses or workshop events with country representatives and LEAs; public campaigns to increase awareness of current provisions and best practice; other activities to help LEAs develop IT tools and human resources. Given that Member States are not required to participate in training and cooperative efforts, it is not possible to assess the extent to which these actions would be taken up by LEAs. The impact of the efforts required in this measure on EU institutions could be small, compared to the baseline
	Simplification benefits		The proposed measure (to improve implementation and enforcement of current provisions) is unlikely to lead to the harmonisation of different national approaches or developing a single procedure for all Member States in case of cross-border cases. The differences would remain, although information about these differences would be better available (through a guidebook and implementation report, communication campaigns, training courses or IT tools).
Fundamental rights		► Personal data protection;	Similar impact as in the baseline.
		► Right to liberty and security	Similar impact as in the baseline.
		► Freedom to conduct business;	Similar impact as in the baseline.

www.parlament.gv.at

1: Improve implementation		
	► Consumer protection	Minor improvements in consumer protection can be expected due to reinforced prosecution of non-cash payment fraud crimes, although the unchanged scope of the legislation limits the magnitude of this impact. The main beneficiaries of this change would be **individual customers**.
	► Right to an effective remedy, in particular the remedies available before the courts.	Similar impact as in the baseline.
EU added value		Better sharing information and best practices, guidance, training and communication campaigns could facilitate cooperation in cross-border cases, compared to the baseline scenario, and it is unlikely to be achieved at the same scale by Member States acting alone. However, the magnitude of this added value is likely to be limited to the scope of current legislation

www.parlament.gv.at

2: Include self-regulatory framework			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	The Commission communication on self-regulatory framework is unlikely to effectively address the general objectives.

www.parlament.gv.at

2: Include self-regulatory framework			
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD2:** PSD2 sets up harmonised requirements needed to ensure that necessary, sufficient and comprehensible information is given to the payment service users with regard to the payment service contract and the payment transactions. PSD2 sets up the transparency of conditions and information requirements for payment services (under Title III) and provides the information about the rights and obligations of payment service users and payment service providers in relation to the provision of the services (under Title IV). Overall, PSD2 ensures that necessary, sufficient and comprehensible information is available regarding the payment transactions and services and about the rights and obligations of payment service users and payment service providers. **Directive on attacks against information systems:** The Directive also refers to fostering and improving the cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. The objective is to receive the support for preserving the evidence, in helping to identify offenders and in shutting down, completely or partially, the information systems or functions that have been compromised or used for illegal purposes. The Directive also promotes the increase of the awareness of innovative SME enterprises to threats relating to such attacks and their vulnerability to such attacks, due to their dependence on the proper functioning and availability of information systems and often limited resources for information security. Overall, the Directive aims to improve the public-private cooperation and promotes the need to increase the awareness of innovative SMEs to threats and vulnerabilities to such attacks. **Directive on Euro counterfeiting:** The Directive aims to strengthen the fight against the criminal conduct and to improve investigation and cooperation against counterfeiting. **Regulation on interchange fees for card-based payment transactions:**

www.parlament.gv.at

2: Include self-regulatory framework			
			The Regulation promotes the use of electronic payments instead of cash payments between the merchants and consumers. The card-based payment transactions are considered beneficial with the condition that the fees for the use of the payment card schemes are set at an economically efficient level. It supports fair competition, innovation and market entry of new operators. Overall, the Regulation promotes the use of non-cash payment instruments. **NIS Directive:** According to Art.15, Member States have to ensure that the competent authority has the necessary powers and means to assess the compliance of operators of essential services. The cooperation between the public and private sectors is essential, as most of the networks and systems are private. Moreover, Art. 15(4) states that the competent authority works in close cooperation with data protection authorities when addressing incidents resulting in personal data breach. Overall, the Directive aims to improve the public-private cooperation. It also envisages the close cooperation between designated authorities and data protection authorities. **Directive on Victims' rights:** The Directive also indicates the obligations of the Member States to take appropriate action, including through the internet, for raising the awareness of the consumers in respect to the negative impact of crime and the risks of victimisation, intimidation and retaliation. Moreover, the Directive emphasizes the enhancement of the cooperation with relevant civil society organisations and other stakeholders.

www.parlament.gv.at

2: Include self-regulatory framework			
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	The Commission communication would likely facilitate self-regulation through public-private partnerships agreements. It is expected that LEAs would participate in such agreements along other stakeholders and they would gain access to (better) information and best practice. For example, reporting non-cash payment fraud can be facilitated through such agreements with other relevant stakeholders. As a result, LEAs capacity to address criminal activity could increase. However, compared to measure 1 this improvement could be more limited, due to lack of legal certainty of self-regulatory framework and possible different interpretations adopted by public-private partnerships agreements, especially if they are adopted at the national level. The main stakeholder group affected by this would be **LEAs, national bank federations and economic operators, potentially also EU institutions, if the framework is adopted at the European level.**
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	Sharing information and best practices among private and public stakeholders could help investigations and prosecutions if relevant authorities are involved, as it is the case in Action Fraud UK which includes participation of the police and victims' organisations. Such (new) agreements could be more effective than the baseline where a limited number of these agreements already exist and are voluntary. For these reasons the expected impact of this measure is likely to be smaller compared to measure 1. The following stakeholder groups are likely to be affected by this measure: LEAs, national bank federations, economic operators, EU institutions, victims associations.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Impacts are likely to be comparable to measure 1.

www.parlament.gv.at

2: Include self-regulatory framework			
		► Increasing protection for victims of non-cash payment fraud;	Compared to measure 1 the improvements in the protection of victims could be smaller due to the fact that public-private partnerships agreements would be voluntary and may continue to have a fragmented geographical scope. The stakeholders most likely to benefit from this are **private sectors representatives (economic operators)**.
		► Stronger cooperation between public institutions/private sector.	The Commission communication aims to facilitate self-regulatory framework for public-private cooperation. Sharing information and best practice within (newly established) public-private partnerships could improve the level of cooperation among the partners but the main limitation of this measure is its voluntary character. The magnitude of this change is therefore likely to be higher than measure 1 and yet moderate. The main stakeholders affected by this change are **LEAs, private sectors representatives, banking federations, victim associations, EU institutions** and **public-private partnerships**.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	A Commission communication for facilitating self-regulatory framework for public-private cooperation would likely bring similar (limited) effects compared to the baseline in terms of increased consumption and trade flows measured by the number and volume of non-cash payment transactions. Compared to measure 1 (Improved implementation) the impacts of measure 2 are likely to be more limited. This is because the levels of consumers' trust in digital purchases would be unlikely to be affected by either the Commission communication, or the resulting public-private partnerships agreements, given the voluntary character of such agreements, their fragmented coverage and often limited effectiveness. Therefore, the expected impact would be small. The same stakeholders as in the baseline would be affected.

www.parlament.gv.at

2: Include self-regulatory framework			
		► Increasing consumer choice due to reduction of fraud	The Commission communication could incentivise the creation of public-private partnerships between relevant actors (from the financial services industry, law enforcement and other stakeholders such as merchants at the national or European level). If taken up, these partnerships could improve the exchange of information and best practices between the public and private sector. Improved information and best practices could help reduce the level of fraud (and thus reduce negative impacts for individual consumers). However, the impact of these activities on consumer choice and reduction of fraud could be limited: slightly lower than the baseline and comparable to measure 1 (improved implementation). While the level of fraud would continue to grow because many areas would remain unprotected, this trend could be a little slower than in the baseline The same stakeholders as in the baseline would be affected, albeit to a smaller extent.
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	This measure is more likely to bring more benefits to economic operators compared to baseline, given that new public-private partnerships by definition would include a representation from the private sector (financial service industry, bank federations, merchants, etc.) As such, the position of economic operators could be better protected (in areas where such agreements are reached) and subsequently bring them reductions in the costs of protecting against fraud. As a result, the level of fraud (and the costs of protection against fraud) could continue to grow albeit slower than in the baseline and comparable to measure 1. The same stakeholders as in the baseline would be affected, albeit to a smaller extent. This measure could be beneficial for economic operators in general. It would be important to ensure that SMEs are sufficiently represented the new public-private partnerships agreements.

www.parlament.gv.at

2: Include self-regulatory framework			
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	The Commission communication on self-regulatory framework could bring very limited administration burden compared to measure 1. This is because required investment would be limited to: - one-off costs for the EU to develop and publish the communication - one-off costs for interested stakeholders to set up public-private partnerships agreements and - continuous (though very limited) costs for these stakeholders to participate in these agreements. Given that it is not mandatory for stakeholders to participate in these efforts, it is not possible to assess the extent to which these actions would be taken up. The impact of the efforts required in this measure on EU institutions could be higher than for baseline, but comparable to those of measure 1.
	Simplification benefits		Similar to measure 1, the Commission communication on self-regulatory framework is unlikely to lead to the harmonisation of different national approaches or developing a single procedure for all Member States in cross-border cases. The differences would remain, although information about these differences would be better available (e.g. in particular for the newly established public-private partnerships agreements). On the other hand, self-regulatory frameworks may actually increase the lack of legal certainty around the issues left out for self-regulation, especially if interpretations among different public-private partnerships agreements at the national level differ.
Fundamental rights		► Personal data protection;	Similar impact as in the baseline (public-private partnerships agreements can rely on existing legislation governing data protection)
		► Right to liberty and security	Similar impact as in the baseline.
		► Freedom to conduct business;	Similar impact as in the baseline.

www.parlament.gv.at

2: Include self-regulatory framework		
	► Consumer protection	Same impact as in measure 1.
	► Right to an effective remedy, in particular the remedies available before the courts.	A further Commission communication on self-regulatory framework would improve the implementation of the Consumer Rights' Directive 2011/83/EU and of the Victims' Directive in the context of increasing the knowledge and awareness of the consumers in respect to risks and vulnerabilities to non-cash payment fraud (right to understand) and ensuring a more efficient use of the public-private partnerships instruments. Moreover, the efficiency of the communication on self-regulatory framework would ensure better protection of the consumer by the Member States authorities against non-cash payment fraud (Art. 38 of the EU Charter), as well as a higher understanding from the victims in an earlier detection of fraud and of his/her rights when submitting complaints, when participating in criminal proceedings and/or trial.
EU added value		It is not clear how effective the Commission communication would be in incentivising voluntary public-private partnerships agreements. Also, a number of such agreements already exist, so compared to measure 1 the added value of this measure is likely to be even more limited. Where the value could be still added is the governance of such agreements in terms of e.g. liability, management of shared information

www.parlament.gv.at

3: Include technology neutral definitions			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure responds to both general objectives: - firstly, a single, technology-neutral definition of non-cash payment would address new forms of fraud, thereby enhancing security - secondly, by addressing these new types of fraud, this measure would raise consumers' trust in non-cash payment transactions and digital single market Overall, this measure would be well aligned with and could address the objectives.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD 2** PSD 2 provides the definition of the payment instrument (Art. 4 para. 1 point 14), as "any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider (PSP) and used in order to initiate a payment order". The concept covers both corporeal and uncorporeal means, while the Framework Decision refers only to the corporeal instruments. Overall, PSD 2 provides the definition of the payment instrument covering both corporeal and uncorporeal means. **Directive on attacks against information systems**: N/A **Directive on Euro counterfeiting:** N/A **Regulation on interchange fees for card-based payment transactions:** The Regulation defines "payment instrument" as any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order (similarly to PSD2 definition); and the "card-based payment instrument" as any payment instrument,

www.parlament.gv.at

3: Include technology neutral definitions			
			including a card, mobile phone, computer or any other technological device containing the appropriate payment application which enables the payer to initiate a card-based payment transaction which is not a credit transfer or a direct debit. Overall, the Regulation defines the payment instrument (as in PSD2) and the card-based payment instrument. **NIS Directive:** N/A **Directive on Victims' Rights:** N/A
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	This option provides LEAs with a legal basis to address criminal activity related to new forms of non-cash payment fraud although it does not directly help increase their enforcement capacity from an operational point of view.
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	With a new legislation (and a broad definition of non-cash payment as well as a crime) the chances of detecting, prosecuting and sanctioning criminals could increase. This is because some forms of possible crimes are not (effectively) prosecuted, since they are not covered or only partially covered by current legislation. Also, this change would be effective over a long period of time, especially if the definition is technology-neutral (i.e. not sensitive to future trends, non-cash means of payment and new forms of fraud). If the definition is too broad and leaves room for interpretation of what the crime is, it could create some issues in cross-border cooperation, in which case the improvement compared to the baseline could be moderate. The main stakeholder group affected by this would be LEAs, judicial representatives and legal practitioners.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	A new and possibly broader definition of non-cash payment fraud could be a moderate deterrent in preventing fraud. The stakeholder groups affected by this measure include individual consumers and economic operators.

www.parlament.gv.at

3: Include technology neutral definitions			
		► Increasing protection for victims of non-cash payment fraud;	The new definition, especially if it is technology-neutral, would provide wider protection from fraud, including new forms of non-cash payment fraud, over a long period of time (i.e. with no need for updating the legislation for any new technological developments or forms of fraud crime). Among the stakeholders affected by this measure are individual consumers and economic operators.
		► Stronger cooperation between public institutions/private sector.	A new definition on its own is unlikely to affect the level of cooperation between relevant actors. This level is likely to remain in line with the baseline.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	Extending substantive criminal law rules to address new forms of non-cash payment fraud by developing a technology-neutral definition of payment instruments and a broad definition of crimes would widen the coverage of existing legislation. This could help build trust in non-cash payment transactions and translate into increased consumption and trade flows measured by the number and volume of non-cash payment transactions. The same stakeholders would be affected as in the baseline (individual consumers and economic operators).
		► Increasing consumer choice due to reduction of fraud	A new definition of non-cash payment (especially if it is technology-neutral), could improve consumer exposure to non-cash payment fraud and the level of fraud could drop, especially around payment fraud on the internet and fraud related to other payment channels and new forms of fraud (e.g. social engineering). This is because some of the measures that could be introduced (e.g. against trafficking of credentials, identity theft or banking malware and money mules) could reduce risks of financial losses for individuals. The same stakeholders would be affected as in the baseline (individual consumers).
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim	Given that the payment industry is a key target of non-cash payment fraud, the positive gains for this group could be higher than for individual consumers and also favourable compared to the baseline. The same stakeholders would be affected as in baseline (economic operators, especially big companies, such as card issuers that bear most of the costs but

www.parlament.gv.at

3: Include technology neutral definitions			
		of the fraud;	benefits are likely to spill over to other firms, including SMEs, as the cost of doing business could be reduced).
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	New legislation could increase administrative burden for the EU institutions and Member States compared to the baseline. This is mainly due to: - one-off costs for the EU: developing a new definition (drawing on and potentially expanding the PSD2 definition) - one-off costs for Member States: adopting this new definition in their national settings - continuous costs for Member States: implementing a wider substantive scope of the Framework Decision Given that a number of Member States have already adopted the PSD2 definition, and that new provisions could build on existing examples, the administrative and financial impacts could be moderate.
	Simplification benefits		This measure could directly respond to limitations uncovered by the evaluation (i.e. lack of widespread national provisions addressing new types of payment instruments and new forms of fraud and discrepancies between national legislation hampering extraterritorial investigations). However, an all-encompassing, technology-neutral definition: - could be more difficult to transpose to national legislation in countries where a detailed definition was adopted - could be open to diverse interpretations, limiting the simplification benefits. Overall, the simplification benefits of this measure could be small .
Fundamental rights		► Personal data protection;	Similar impact as in the baseline.
		► Right to liberty and security	The new definition would have a positive impact on the right to security by regulating forms of non-cash payment not covered by current legislation and improving chances for prosecuting fraud criminals and better protecting victims of fraud crimes.
		► Freedom to conduct	Similar impact as in the baseline.

www.parlament.gv.at

3: Include technology neutral definitions		
	business;	
	► Consumer protection	With a new, technology-neutral and all-encompassing definition of non-cash payment and crimes, there could be a notable improvement in consumer protection. This is because several forms of possible crimes (e.g. acting as a money mule, trafficking of credentials, skimming, sniffing, trashing, and identity theft) that are not covered or only partially covered by the Framework Decision and the national laws could be covered by the new definition.
	► Right to an effective remedy, in particular the remedies available before the courts.	Member States should ensure that the principles of legality and proportionality of criminal offences and penalties is respected.
EU added value		A new definition at EU level would capture new forms of non-cash payment fraud and it would likely improve cross-border investigations and prosecutions.

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure responds to the first general objective by criminalising preparation for fraud & better data protection and thus improving security and trust in non-cash payment transactions.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD2:** It contains the following provisions related to preparatory acts: - unauthorised access to a payment instrument; - illegal use of sensitive and personal data. Art. 103 of PSD 2 leaves to the Member States to set up the rules on penalties applicable to infringements of the national law transposing the Directive and to ensure that these penalties are effective, proportionate and dissuasive. The competent authorities have the power to disclose to the public any administrative penalty that is imposed for infringement, unless such disclosure would seriously jeopardize the financial markets or cause disproportionate damage to the parties involved. PSD2 does not provide information about the minimum maximum level of penalties. In addition, the penalties in the PSD2 are not criminal sanctions (PSD2 is not a criminal law instrument). **Directive on attacks against I.S.:** Article 7 of the Directive mentions the tools used for committing offences. Thus, “the intentional production, sale, procurement for use, import,

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences			
			distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Art. 3 to 6, is punishable as a criminal offence, at least for cases which are not minor: (a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Art. 3 to 6; (b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed. **Directive on Euro counterfeiting:** This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of counterfeiting of the euro and other currencies. Overall, this Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of counterfeiting of the euro and other currencies. No information about preparatory conduct. **Regulation on interchange fees for card-based payment transactions:** Art. 14 of the Regulation leaves to the Member States the decision to set up the penalties applicable to infringements of the Regulation in that Member States and to ensure that these penalties are effective, proportionate and dissuasive. **NIS Directive:** There is no provision for criminalisation the preparatory acts. **Directive on Victims' Rights**: N/A
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	The criminalisation of preparatory acts could directly affect the capacity of LEAs, as this measure could expand the number of fraud cases to be investigated. The measure could cover conduct such as phishing, stealing data, money mules and identity theft, which are inconsistently addressed by current legislations. The main stakeholder group affected by are LEAs, judiciary representatives and legal practitioners.

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences			
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	The criminalisation of preparatory acts would enable their investigation and prosecution. Compared to the baseline this measure could have significant effects, in particular on enhancing security. The main stakeholders affected are LEAs, judiciary representatives and legal practitioners.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	The criminalisation of preparatory acts could prevent fraud from taking place and limit organised crime gains. Compared to the baseline this measure could have significant effects. The main stakeholders affected are individual consumers and economic operators.
		► Increasing protection for victims of non-cash payment fraud;	Criminalising conduct preparatory to or supportive of fraud and setting a minimum level of sanctions for these could improve the level of protection for victims of non-cash payment. Compared to the baseline this measure could have significant effects. The main stakeholders affected are individual consumers and economic operators.
		► Stronger cooperation between public institutions/private sector.	The criminalisation of preparatory acts is unlikely to significantly affect the level of public-private cooperation, compared to the baseline scenario.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	This measure could positively affect the level of trust of non-cash payment transactions, as it would contribute to better protect individual customers and economic operators from fraud (i.e. regardless, if the fraud occurred and if it generated financial losses for the victim). This could contribute to increase consumption compared to the baseline. The same stakeholders would be affected as in baseline (individual consumers and economic operators).
		► Increasing consumer choice due to reduction of fraud	Setting minimum level of sanctions for fraudulent activities and criminalising conduct preparatory to or supportive of fraud could lead to an improvement in consumer protection. The same stakeholders would be affected as in baseline (individual consumers).

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences			
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	This measure could reduce the level of fraud and increase cost-savings for economic operators. These gains could reduce the cost of doing business and spill over to other firms, including SMEs. The same stakeholders would be affected as in baseline (economic operators, including SMEs).
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	Setting a minimum level of sanctions for fraudulent activities and criminalising conduct preparatory to or supportive of fraud could increase administrative burden for EU institutions and Member States, through: - one off costs for the EU for developing new legislation - one off costs for MS for adopting new provisions to their national systems - continuous costs for MS: implementing new legislation, which could increase the number of cases for investigation. Overall, the cumulative impact of this measure on administrative and financial costs could be higher than in the baseline. Increased number and scope of investigations of fraud crimes would mainly affect LEAs, judiciary, legal practitioners.
	Simplification benefits		This measure could set a minimum level of sanctions for the maximum penalty. At the same time it would leave the flexibility for Member States to regulate the upper ceiling, as well as minimum penalty levels. Minimum levels of sanctions could ensure a more coherent treatment of fraud criminals across MS. This measure could have a higher impact compared to baseline.
Fundamental rights		► Personal data protection;	Stealing of data, trafficking credentials and similar conduct preparatory to fraud would be criminalised. This could complement the security and data breach rules to create better personal data protection compared to the baseline scenario.
		► Right to liberty and security	The minimum sanctions would have a positive impact on the right to security by criminalising conduct preparatory to fraud, improving chances for prosecuting fraud criminals and better protecting victims.

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences		
	► Freedom to conduct business;	Similar impact as in the baseline.
	► Consumer protection	This measure could have a positive impact on consumer protection through the criminalisation of preparatory acts.
	► Right to an effective remedy, in particular the remedies available before the courts.	Similar impact as in the baseline.
EU added value		The criminalisation of preparatory acts at EU level would ensure coherence legislation across Member States, including with regards to the levels of penalties for these offences, which could have a positive impact in cross-border cooperation.

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure is coherent in particular with the general objective of enhancing security, as updated jurisdiction rules are likely to enhance investigation and prosecution.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	This measure complies with Directive 2013/40/EU on attacks against information systems, and in particular with Art. 12, which establishes the jurisdiction rules applicable to Member States. According to that Article, Member States establish their jurisdiction when the offence has been committed: (a) in whole or in part within their territory either in case the offender commits the offence when physically present on its territory (whether or not the offence is against an information system on its territory) or in case the offence is against an information system on its territory (whether or not the offender commits the offence when physically present on its territory), OR (b) by one of their nationals, at least under the condition that the conduct is incriminated in the legislation of the state where the offence was committed. This policy measure could be also in line with the Council Framework Decision 2008/841/JHA on the fight against organized crime, which states at Art. 7 the rules for settlement of jurisdiction and coordination of prosecution of transactional organised crimes cases. The Framework Decision envisages that Member States may have recourse to Eurojust or other body or mechanism established within the European Union for

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive			
			facilitating the cooperation between the judicial authorities. For this purpose, the Framework Decision states that the following factors shall be taken into consideration when related to the Member States involved: the Member State in the territory of which the acts were committed; the Member State of which the perpetrator is a national or resident; the Member State of the origin of the victims; the Member State in the territory of which the perpetrator was found. This measure also is in line with the Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings. The decision aims to prevent any infringement of the principle of "ne bis in idem", where the same person is subject to parallel criminal proceedings in different Member States for commission of the same acts that constitute offences. Moreover, the Framework Decision establishes the rules for reaching consensus on the effective solutions for avoiding adverse consequences arising when parallel proceedings occur. This measure is complemented by the Directive (EU) 2016/680, which assures harmonized rules for the protection and the free movement of personal data processed with the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, these rules applying also in cross-border cases. Moreover, this measure would support the application of both the Regulation (EU) 2016/794 on Europol (on strengthening the Europol' role of providing support to the Member States in preventing and combating serious crime affecting two or more Member States) and of Council Decision 2009/426/JHA on the strengthening of Eurojust (in which Eurojust plays a strategic role in facilitating the cooperation between two or more competent authorities of the Member States and the coordination of their action, including in supporting the cases where conflicts of jurisdiction have arisen or are likely to

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive			
			arise).
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	This measure would not directly affect law enforcement capacity to address fraud crimes: while the new provisions would update the jurisdiction rules, there are no additional provisions to address capacity issues of LEAs (i.e. on additional resources made available to LEAs).
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	The chances of detecting, prosecuting and sanctioning of fraudsters could likely improve through the updated jurisdiction rules. The stakeholders mostly concerned with this measure include individual consumers, economic operators, LEAs, judiciary representatives and legal practitioners.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Establishing jurisdiction in non-cash payment fraud cases can be a complex issue, especially when the crime is committed in (or using) an IT system located in a country different than the offender, where evidence is in the cloud or in an unknown place. This measure would facilitate the process of establishing jurisdiction for Member States affected. This is likely to lead to increased detection, prosecution and sanctioning of offenders. More effective sanctioning could further act as better deterrence. The impact of this measure compares favourably against the baseline. The stakeholders most concerned include individual consumers and economic operators.
		► Increasing protection for victims of non-cash payment fraud;	Through updating the jurisdiction rules, a larger number of complex cross-border cases could be investigated, which in turn is likely to increase the level of protection for victims of non-cash payment fraud, compared to the baseline. The stakeholders most concerned include individual consumers and

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive			
			economic operators.
		► Stronger cooperation between public institutions/private sector.	This measure is not expected to affect the level of cooperation between public institutions and private sector (e.g. banks and police), since it is limited to establishing jurisdictions and concerns primarily judicial authorities.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	The evaluation found there are still issues in identifying the competent jurisdiction over complex cross-border cases, especially where the territoriality principle becomes insufficient (e.g. crime evidence stored in the cloud). These cases are not specifically addressed by the current Framework Decision leaving many crimes unpunished. This measure could address legal (but not necessarily practical) reasons for dropping such cases and improve deterrence, thus indirectly contributing to improved consumer trust in non-cash payment. The increase might be higher compared to baseline. The stakeholders affected include **individual consumers** and **economic operators.**
		► Increasing consumer choice due to reduction of fraud	The new measure is likely to improve deterrence by updating the rules on 'online' jurisdictions and reducing fraud. This could translate into economic gains and reduce (or freeze) fraud margins and costs of (credit / debit) cards set up by merchants. This is likely to increase consumer choice compared to the baseline. The stakeholders affected include **individual consumers**.
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	This measure is likely to improve protection and cost-savings for economic operators that are victims of fraud since it updates the rules on jurisdictions in complex cross-border cases (which are often dropped today for legal and practical reasons). In the long term businesses are likely to see some gains following the expected reduction of fraud, albeit on a

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive			
			limited scale. The reduction of fraud would turn into cost-savings for economic operators as they may be spending less on protecting against fraud - improvement compared to the baseline. The stakeholders affected include **economic operators.**
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	It is expected that this measure would increase administrative burdens for EU institutions and Member States due to: - one off costs for the EU for developing the new legislation - one off costs for Member States for adopting new provisions to their national settings - continuous costs for the EU: facilitating cooperation among all affected Member States through Eurojust - continuous costs for MS: cooperation with all affected Member States & centralising proceedings in a single MS. Overall, the cumulative impact of this measure on administrative and financial costs could be higher than in the baseline. The stakeholders affected include **LEAs and EU institutions.**
	Simplification benefits		The international dimension of non-cash payment fraud requires cooperation between Member States and this measure aims to clarify rules on substantial jurisdiction and facilitate cooperation among Member States affected. This shows improvement over the baseline.
Fundamental rights		► Personal data protection;	By providing for enhanced access to justice for victims of fraud, this measure would enhance the protection provided by criminal law in cases involving violation of privacy. The measure would therefore have a limited positive impact compared to the baseline.
		► Right to liberty and security	The measure would have a positive impact on the right to security by providing victims of fraud with enhanced access to

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive		
		the protection provided by criminal law
	► Freedom to conduct business;	No significant impact.
	► Consumer protection	This measure is likely to improve consumer protection by clarifying rules on jurisdictions and making it easier to pursue complex cross-border fraud cases. This compares favourably to the baseline.
	► Right to an effective remedy, in particular the remedies available before the courts.	The measure would have a positive impact on the right to an effective remedy by enhancing access of victims of fraud to the protection provided by criminal law
EU added value		In the area of cross-border cooperation this measure would address the current gap in the Framework Decision in cases where jurisdiction is not clear. The evaluation showed that currently these cases are often dropped for legal and practical reasons. This measure is likely to address the former - for this reason its added value is small, but better than the baseline.

www.parlament.gv.at

8: Extend jurisdiction rules to complement the European Investigation Order			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure directly addresses the strategic policy objective of enhancing security, as it would likely improve investigation and prosecution.
	External coherence with relevant existing EU legislation	In particular: ► European Investigation Order;	**European Investigation Order:** The EIO aims at ensuring the mutual recognition of decisions taken to obtain evidence. This measure would complement the EIO, as it would provide training and have the issuing authority provide feedback to the executing authority about the use made of the evidence provided and about the outcome of the prosecution.
Effectiveness	**Social impacts**	► Increasing law	This measure would affect law enforcement capacity to address fraud

www.parlament.gv.at

8: Extend jurisdiction rules to complement the European Investigation Order			
		enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	crimes by including rules to complement the EIO on better preparing contact points for carrying out their task through training and feedback loops. This in turn could make the EIO processes more efficient and overcome some obstacles to cross-border investigations.
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	The chances of detecting, prosecuting and sanctioning fraudsters could be largely improved by including rules to complement the EIO. These rules could reassure stakeholders at national level about their ability to request and receive electronic evidence, allowing investigators and prosecutors to obtain the required data for their case more efficiently.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Similarly to 'Improved implementation' (measure 1), this measure is likely to bring down the number of criminal acts and organised crime gains related to new forms of payment fraud, since it would allow for more efficient enforcement of current provisions.
		► Increasing protection for victims of non-cash payment fraud;	By complementing the EIO, the work of investigators and prosecutors could be more efficient, which in turn could increase the level of protection for victims of non-cash payment fraud.
		► Stronger cooperation between public institutions/private sector.	This measure is likely to affect the level of cooperation between public institutions and private sector, since it could enhance existing cooperation mechanisms.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	The use of non-cash payments might further increase, as trust in and security of non-cash payment transactions could benefit from rules complementing the EIO (to facilitate cross-border cooperation by making the most of the existing mechanisms).
		► Increasing consumer choice due to reduction of fraud	Complementing the EIO could lead to some improvements in consumer protection and the level of fraud could fall. This could translate into economic gains. Since merchants may pass on the costs of fraud to consumers, with increased trust and protection the prices could decrease. The costs of (credit / debit) cards are likely to go down for the same reason

www.parlament.gv.at

8: Extend jurisdiction rules to complement the European Investigation Order			
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	Including rules to complement the EIO is likely to improve protection and cost-savings for economic operators that are victims of fraud since the information exchange needed to prosecute perpetrators could be easier. While these savings would be more relevant to actors other than economic operators, in the long term businesses could also see some gains following the expected reduction of fraud, albeit on a limited scale. The reduction of fraud could turn into cost-savings for economic operators as they may not need to spend as much to protect against fraud.
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	This measure could marginally increase administrative burdens for EU institutions and Member States, through the following costs: - continuous costs for the EU: training for contact points (assuming training is carried out at the EU level) - continuous costs for Member States: increased number of EIO requests and feedback to the executing authority. Overall, the cumulative impact of this measure on administrative and financial costs could be only slightly higher than in the baseline Increased number and scope of investigations of fraud crimes could mainly affect LEAs, judiciary, legal practitioners. This measure could also affect EU institutions.
	Simplification benefits		The international dimension of non-cash payment fraud requires cooperation between Member States and faces a number of barriers that the rules complementing the EIO could address (e.g. in identifying the responsible Member States for offences affecting more than one Member State). The main advantage of this measure is that it seeks to improve efficiency of existing mechanisms for cooperation but as such its simplification benefits are relatively small.
Fundamental rights		► Personal data protection	Respect of data protection rules is paramount both for law enforcement when sending requests and for the addressees of those requests, when responding to them. Appropriate safeguards must be in place, in accordance with existing data protection rules.

www.parlament.gv.at

8: Extend jurisdiction rules to complement the European Investigation Order		
	► Right to liberty and security	The measure could have a positive impact on the right to security by enhancing effectiveness of law enforcement action.
	► Freedom to conduct business;	No significant impact.
	► Consumer protection	This measure ensures the protection of exchanged data (also when personal data is shared) but bears some risks of excessive use of investigative powers. To mitigate these risks, the measure could include additional procedural safeguards.
	► Right to an effective remedy, in particular the remedies available before the courts.	Safeguards are already enshrined within the EIO, with which this policy measure would be consistent.
EU added value		In the area of cross-border cooperation this measure could add some value to what is already in place and what Member States could have achieved by acting on their own. The evaluation found that exchange of information and cooperation between law enforcement and judicial authorities of different countries is increasingly necessary in investigations and prosecutions. However, different national standards on the admissibility of evidence can prevent the investigations from continuing. This measure aims to facilitate investigations and prosecutions by leveraging existing mechanisms.

www.parlament.gv.at

9: Adapt rules on injunction for cooperation/evidence purposes			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure directly addresses the general objective of enhancing security.
	External coherence with relevant existing EU legislation	In particular: ► Policy process on improving cross-border access to electronic evidence in criminal matters	**Improving cross-border access to electronic evidence in criminal matters**: This ongoing process is to lead to measures aiming at tackling a number of problems that have been identified as relevant in the area of non-cash payment fraud. This policy measure would need to be complementary to future initiatives to improve cross-border access to electronic evidence.
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	This measure could improve law enforcement capacity through a facilitated access to the evidence for prosecution purposes.

www.parlament.gv.at

9: Adapt rules on injunction for cooperation/evidence purposes			
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	The chances of detecting, prosecuting and sanctioning fraudsters could be improved through adapting the rules on injunctions, as these would address both substantive and procedural law. These rules could facilitate cross-border investigations and prosecutions, therefore making the process of bringing perpetrators to justice more effective and efficient.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Similarly to 'Improved implementation' (measure 1), this measure could bring down the number of criminal acts and organised crime gains related to new forms of payment fraud, since it could allow for a more effective and efficient enforcement of current provisions.
		► Increasing protection for victims of non-cash payment fraud;	Through adapting the rules on injunctions the work of investigators and prosecutors could be easier and more efficient which in turn could increase the level of protection for victims of non-cash payment fraud.
		► Stronger cooperation between public institutions/private sector.	This measure could reinforce cooperation between public institutions and the private sector.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	The use of non-cash payments might further increase, as trust in and security of non-cash payment transactions could benefit from adapted rules on injunctions. In particular, this measure could facilitate and speed up law enforcement action against criminal activities infringing consumers' and victims' rights.
		► Increasing consumer choice due to reduction of fraud	This measure would enable Member States to issue injunction orders for cooperation. Assuming effective law enforcement and execution, this could improve consumer protection and the level of fraud could fall. This could translate into economic gains. Since merchants may pass on the costs of fraud to

www.parlament.gv.at

9: Adapt rules on injunction for cooperation/evidence purposes			
			consumers, with increased trust and protection, the prices could decrease. The costs of (credit / debit) cards to consumers and/or merchants are likely to go down for the same reason
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	Injunctions could allow Member States to facilitate cooperation and cross-border prosecutions. This could improve protection and cost-savings for economic operators that are victims of fraud. While these savings would be more relevant to actors other than economic operators, in the long term businesses could also see some gains following the expected reduction of fraud, albeit on a limited scale. The reduction of fraud would turn into cost-savings for economic operators as they may be spending less on protecting against fraud.
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	This measure could facilitate cooperation in cross-border fraud cases. At the same time, it would require the application of decisions taken by courts and administrative authorities of Member States A in Member States B, thus increasing the level of cooperation between member states' authorities.
	Simplification benefits		The international dimension of non-cash payment fraud requires cooperation between Member States. This measure could facilitate the application of decisions taken by courts and administrative authorities of a Member State A in a Member State B and increase the efficient administration of criminal justice in cross-border cases.
Fundamental rights		► Personal data protection;	Respect of data protection rules is paramount both for law enforcement when sending requests and for the addressees of those requests, when responding to them. Appropriate safeguards must be in place, in accordance with existing data protection rules.
		► Right to liberty and security	The measure would have a positive impact on the

www.parlament.gv.at

9: Adapt rules on injunction for cooperation/evidence purposes		
		right to security by enhancing effectiveness of law enforcement action
	► Freedom to conduct business;	No significant impact.
	► Consumer protection	No significant impact.
	► Right to an effective remedy, in particular the remedies available before the courts.	Accessing evidence across borders could help effective detection and prosecution of crimes, and the protection of victims of crime. At the same time, measures to facilitate cross-border access to evidence, may raise questions of impact on fundamental rights. Any legislative initiative must respect the right to fair trial and include safeguards to protect the rights of the persons affected, including the rights of the defence, the right to an effective remedy as well as other procedural rights.
EU added value		In the area of cross-border cooperation this measure would be unlikely to be replaced by similar arrangements between 28 Member States.

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure responds to the second general objective by better protecting natural and legal persons and reinforcing their trust in non-cash payment and the digital single market
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD2:** PSD2 sets up the conditions where the different actors in the payment process are held liable. As such, the payment service provider is held liable for unauthorized payment transactions (Art. 73) and has the obligation to refund the payer the amount of the transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. The payer is liable for unauthorized payment transactions (Art. 74) and he/she may be obliged to bear the losses relating to any unauthorized payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. No reference to identity theft is made.

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft			
			Directive on attacks against information systems: The Directive calls for setting up effective measures against identity theft and other identity-related offences, as this constitutes an important element of an integrated approach against cybercrime. **NIS Directive:** The Directive confirms that personal data are in many cases compromised as a result of incidents and calls for competent authorities and data protection authorities to cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents. **Directive on Victims' Rights:** The Directive defines the 'victim' as: (i) a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence; (ii) family members of a person whose death was directly caused by a criminal offence and who have suffered harm as a result of that person's death. There is no definition of victim that is applied to the legal person. Protecting the privacy of the victim can be an important means of preventing secondary and repeated victimisation, intimidation and retaliation and can be achieved through a range of measures including non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of the victim. There is no reference to specific protection measures against identity theft
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-	Impact comparable with that of the baseline.

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft			
		cash payment fraud;	
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	Impact comparable to that of the baseline.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Impact comparable to that of the baseline. The stakeholder groups affected by this measure include **individual consumers** and **economic operators.**
		► Increasing protection for victims of non-cash payment fraud;	The new provisions aim to substantially improve protection for natural and legal persons who are victims of non-cash payment fraud. Expected impact is likely to be higher than that of the baseline. Among the stakeholders affected by this measure are **individual consumers** and **economic operators**.
		► Stronger cooperation between public institutions/private sector.	Impact on cooperation between public institutions and private sector are likely to remain in line with that of the baseline.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	Additional provisions for protecting natural and legal persons from fraud could help build trust in and security of non-cash payment transactions. There could also be an increase in business-to-business online transactions, especially as regards SMEs. In turn, this would translate into increased consumption and trade flows measured by the number and volume of non-cash payment transactions. The increase could be higher compared to the baseline, given that the scope of protection is extended to legal persons, including SMEs. The same stakeholders would be affected as in baseline (individual consumers and economic operators).

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft			
		► Increasing consumer choice due to reduction of fraud	Impact comparable to that of the baseline. The same stakeholders would be affected as in baseline (individual consumers).
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	This measure would expand the protection to legal persons, including SMEs which are particularly vulnerable to fraud because they may lack of effective cybersecurity systems in place and they may be less likely to have insurance against non-cash payment fraud. This measure could have higher impact for economic operators compared to baseline. The same stakeholders would be affected as in the baseline (economic operators). Given that SMEs form a large proportion of businesses in the EU, this measure could be particularly beneficial for this group.
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	New legislation could increase administrative burden for the EU institutions and Member States, compared to the baseline. This is mainly due to: - one-off costs for the EU: developing new legislation (drawing on and potentially expanding the PSD2 provisions)- one-off costs for adopting new provisions - continuous costs for implementing a wider protection for natural and legal persons; education measures, communication campaigns The administrative and financial impacts could be moderate This measure would primarily affect EU institutions and LEAs.
	Simplification benefits		Impact comparable to that of the baseline.
Fundamental rights		► Personal data protection;	The new rules on assistance to victims of identity theft are expected to complement existing rights and to enhance data protection.
		► Right to liberty and	New provisions protecting natural and legal persons from identity

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft		
	security	theft could have a positive effect on the right to liberty and security, compared to the baseline.
	► Freedom to conduct business;	New provisions protecting natural and legal persons from identity theft could have a positive effect on the freedom to conduct business, as victims of identity theft who are, e.g. merchants, would be better protected from the negative consequences of identity theft.
	► Consumer protection	This option is expected to improve consumer protection for natural persons, complementing PSD2 provisions on compensation;
	► Right to an effective remedy, in particular the remedies available before the courts.	Similar impact as in the baseline.
EU added value		By extending and complementing provisions under the Directive on Victims' Rights, this measure is expected to bring about an enhanced level of protection of victims across the Union.

www.parlament.gv.at

12: Facilitate cross-border cooperation			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	This measure would directly address the general policy objective of enhancing security, by contributing to more effective investigations and prosecutions. It is also likely to reinforce the trust of consumers and economic operators, as it would contribute to enhance law enforcement action on cross-border cases.
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	This measure would comply with the Regulation No 223/2009 on European statistics Eurostat and would allow for maintaining comprehensive statistics on non-cash payment fraud and counterfeiting. This could lead to a better assessment of the effectiveness of the systems in place, identifying trends in non-cash payment fraud, prevention and combating actions needed. Moreover, EU citizens would have access to statistical data on non-cash payment fraud. This measure would complement existing provisions aiming at gathering relevant statistics under the PSD2 and the fourth AML Directive. In terms of strengthening the role of the contact points, this measure would support the application of Regulation (EU) 2016/794 on Europol and of Council Decision 2009/426/JHA on the strengthening of Eurojust, that require Member States to designated contact points for coordination and would be in line with the corresponding provisions under the Directive on attacks against information systems. Moreover, the designation and specialisation of contact points could improve the practice on investigation and prosecution, as well as in the area of mutual legal assistance in criminal matters in terms of process validation, use of investigative techniques, response time and quality of information, as well as on victims' support, in accordance with the EIO Directive, EAW

www.parlament.gv.at

12: Facilitate cross-border cooperation			
			Framework Decision and Injunction Directive. Regarding the incentives of Member States for sharing the information with Europol, the measure is also coherent with Regulation (EU) 2016/794 and would conduct to a development of the Member States' cooperation with Europol in cross-border information exchange activities, operations and investigations.
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	This measure could enhance law enforcement capacity to address fraud by strengthening the role of existing contact points. This measure requires that additional resources be made available to LEAs, also to be able to collect statistics on investigations and prosecutions of non-cash payment offences. The stakeholders affected are mainly LEAs.
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	Facilitating LEAs cooperation, the chances of detecting, prosecuting and sanctioning fraudsters could increase. These measures would incentivise and further facilitate exchange of information. The stakeholders affected include individual consumers, economic operators, LEAs, judiciary representatives and legal practitioners.
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Similarly to 'Improved implementation' (measure 1), this measure could contribute to diminish the number of criminal acts and organised crime gains resulting from non-cash payment fraud, by enhancing the quality of available information and the enforcement of existing provisions. The stakeholders affected include individual consumers and economic operators.
		► Increasing protection for victims of non-cash payment fraud;	More effective contact points could contribute to making cross-border cooperation more efficient, which in turn could increase the level of protection for victims of non-cash payment fraud. Better statistics on investigations and prosecutions would allow to better target law enforcement action. The stakeholders affected include individual consumers and economic

www.parlament.gv.at

12: Facilitate cross-border cooperation			
			operators.
		► Stronger cooperation between public institutions/private sector.	This measure is likely to improve the level of cooperation between public institutions and private sector, by enhancing and increasing available information. –Similarly to measure 8 this would represent an improvement compared to the baseline. The stakeholders affected include economic operators, LEAs, judiciary representatives, economic operators and banking federations.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	The use of non-cash payments might further increase, as trust in and security of non-cash payment transactions would benefit from better prevention of fraud. This would represent an improvement compared to the baseline, comparable to the effects of measure 8. The stakeholders affected include individual consumers and economic operators.
		► Increasing consumer choice due to reduction of fraud	Incentivising sharing information among Member States and clarifying and strengthening the role of dedicated contact points could lead to a reduced level of fraud and consequently improve consumers' protection. This could translate into economic gains. Since merchants may transfer the costs of fraud on to consumers, this measure could have a positive impact on price. The administrative costs associated to the use of non – cash payment instruments could go down for the same reason. The stakeholders affected include individual consumers.
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	This measure is likely to improve protection and cost-savings for economic operators that are victims of fraud since it incentivises information exchange. In the long term, businesses could benefit from the expected reduction of fraud. The reduction of fraud could result in savings for economic operators, which may not need to invest as much on fraud detection and protection. The stakeholders affected include economic operators.

www.parlament.gv.at

12: Facilitate cross-border cooperation			
Efficiency	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	This measure is expected to increase administrative burden for Member States due to: - one off costs for adopting new provisions to their national settings - continuous costs for Member States: collecting statistics on investigations and prosecutions of non-cash payment fraud and designating contact points. The stakeholders affected include LEAs and EU institutions.
	Simplification benefits		The international dimension of non-cash payment fraud requires cooperation between Member States and this measure aims to facilitate cooperation largely drawing on existing mechanisms.
Fundamental rights		► Personal data protection;	This measure does not have substantial impacts compared to the baseline. The exchange of information resulting from these provisions on improving cross-border cooperation would have to be carried out in full compliance with existing data protection rules.
		► Right to liberty and security	New provisions facilitating cross-border cooperation could have a positive effect on the right to liberty and security, as they are likely to enhance cross-border investigations and prosecutions.
		► Freedom to conduct business;	New provisions facilitating cross-border cooperation could have a positive effect on the freedom to conduct business, in particular those that involve cross-border economic activity, since these provisions are likely to provide for a safer business environment by enhancing cross-border investigations and prosecutions.
		► Consumer protection	This measure indirectly improves consumer protection by enhancing information sharing.
		► Right to an effective remedy, in particular the remedies available before the courts.	No significant impact.

www.parlament.gv.at

12: Facilitate cross-border cooperation		
EU added value		This measure would add value to mechanisms in place. Member States acting on their own may not be able to build a network of points of contact with specific common requirements.

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing			
Coherence	**Internal** coherence with the strategic objectives of the intervention	► Enhance security, by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment fraud as a source of income and therefore an enabler of other criminal activities, including terrorism ► Support the digital single market, by increasing consumers' trust and reducing the negative impact on economic activity of non-cash payment fraud	By paving the way towards better information sharing, this measure would contribute to achieve the general objectives, enabling more targeted action by LEAs (enhancing security) and contributing to prevention (increasing trust of consumers).
	External coherence with relevant existing EU legislation	E.g.: ► PSD2; ► Directive on attacks against information systems; ► Directive on counterfeiting of euro; ► Regulation on interchange fees for card-based payment transactions; ► NIS Directive.	**PSD2:** According to Art. 68 para 6, the account servicing payment service provider shall immediately report any incident relating to the account information service provider or the payment initiation service provider to the competent authority. The provider may block and deny the use of the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorized or fraudulent use of the payment instrument. Moreover, PSD2 states that where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds which are communicated to the relevant national authority, the payment service provider should be able to conduct an investigation before deciding to refund the payer. Art. 96 of PSD2 states that "in the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider." Overall, payment service providers have the obligation to report any

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing			
			security incident in connection to the payment instrument and any suspicion of unauthorized or fraudulent use of the payment instrument. There is a need for further guidance on improving the detection of suspicious fraudulent conduct as stated under PSD2. **Directive on attacks against information systems:** Art. 13 para. 3 states that the Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in art. 3 to 6 to the competent national authorities without undue delay. **NIS Directive:** The Directive establishes security and notification requirements for operators of essential services (Article 14) and for digital service providers (Article 16). Entities that do not fall under these categories may notify the incidents, on a voluntary basis. **Directive on Victims' Rights:** Under Art. 5, Member States shall ensure that victims who wish to make a complaint with regard to a criminal offence and who do not understand or speak the language of the competent authority are enabled to make the complaint in a language that they understand or by receiving the necessary linguistic assistance. The Directive states that measures should be in place to make possible the use of communication technology, such as e- mail, video recordings or online electronic forms for making complaints. The authorities of the Member State where the criminal offence was committed shall, in particular, be in a position: (a) to take a statement from the victim immediately after the complaint with regard to the criminal offence is made to the competent authority; (b) to have recourse to the extent possible to the provisions on video

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing			
			conferencing and telephone conference calls for the purpose of hearing victims who are resident abroad. Art. 17 para.2 of the Directive states that Member States shall ensure that victims of a criminal offence committed in Member States other than that where they reside may make a complaint to the competent authorities of the Member State of residence, if they are unable to do so in the Member State where the criminal offence was committed or, in the event of a serious offence, as determined by national law of that Member State, if they do not wish to do so. Moreover, the Member States competent authorities have to take appropriate measures to minimize the difficulties faced where the victim is a resident of a Member State other than that where the criminal offence was committed, particularly with regard to the organisation of the proceedings. The moment when a complaint is made should, for the purposes of this Directive, be considered as falling within the context of the criminal proceedings. This should also include situations where authorities initiate criminal proceedings ex officio as a result of a criminal offence suffered by a victim. Overall, the Directive states the right of the victim to make a complaint about a criminal conduct to the competent authorities of the Member State where he/she resides or in the Member States where the criminal offence was committed or, in the event of a serious offence, as determined by national law of that Member State. The Member States shall put at disposal of the victim the communication technology, such as e-mail, video recordings or online electronic forms for making complaints.
Effectiveness	**Social impacts**	► Increasing law enforcement capacity to address criminal activity related to new forms of non-cash payment fraud;	Compared to the baseline this measure could have positive consequences for the capacity of law enforcement. This is because the reporting provisions could be targeted to the most significant ones (improved quality, rather than quantity of information available), in the case of voluntary reporting. The main stakeholders affected include LEAs.

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing			
		► Increasing chances of prosecuting, sanctioning and detecting criminals;	Voluntary and targeted reporting could increase chances of detecting, prosecuting and sanctioning perpetrators compared to baseline. The main stakeholder groups affected here are LEAs, economic operators, National Banking Federations, individual consumers (victims of fraud).
		► Decreasing number of criminal acts and organized crime gains related to non-cash payment fraud;	Effects of this measure could be higher than in the baseline, due to increase reporting possibly serving as a deterrent. The main stakeholders affected by this measure are individual consumers and economic operators.
		► Increasing protection for victims of non-cash payment fraud;	This measure could marginally increase the protection for victims for non-cash payment fraud due to increased reporting. The main stakeholders affected include primarily economic operators victims of fraud who seek legal certainty over non-cash payment fraud reporting.
		► Stronger cooperation between public institutions/private sector.	The level of co-operation between public institutions and the private sector is also expected to improve due to the new provisions encouraging reporting, as they could add legal certainty that encourages cooperation. The main groups of stakeholders benefiting from these effects include: economic operators, LEAs, National Banking Federations, individual consumers victims of fraud and victims associations.
	Economic impacts	► Increasing consumption and trade flows due to higher consumer trust in digital purchases of goods and services;	New provisions on voluntary reporting could have smaller impact on consumers' trust compared to mandatory reporting.. The affected stakeholders include individual consumers and economic operators.
		► Increasing consumer choice due to reduction of fraud	Given that reporting could be voluntary, the impact on consumer choice are likely to be marginal but still represent an improvement compared to the baseline.

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing			
			The affected stakeholders include individual consumers.
		► Increasing cost-savings for economic operators (i.e. financial services providers, retail goods or services providers) that are the victim of the fraud;	By increasing legal certainty for reporting of non-cash payment fraud, this measure could bring about positive effects on fraud reduction and cost-savings for economic operators. This could represent an improvement compared to the baseline. Reporting could be targeted and economic operators could have an interest in reporting cases of fraud that affect them but which they don't report due lack legal certainty. The affected stakeholders include economic operators.
t	**Financial and administrative costs**	► Increasing/decreasing administrative burdens for public and private sectors	Provisions to encourage reporting are less likely to bring about positive effects in Member States lacking adapted mechanisms, platforms and channels for information sharing. Also, economic operators which are more vulnerable to extra costs and administrative requirements- (in particular SMEs) are less likely to make use of those provisions. As such, the most likely costs associated with this measure include: - one-off costs for the EU: developing new legislation - one off costs for Member States: adopting new provisions to national settings (many Member States already regulated their reporting practices and these might need to be adjusted). - continuous costs for LEAs: creating and maintaining dedicated points of contact to facilitate cooperation across Member States. - continuous costs for economic operators to report targeted non-cash payment fraud cases. Increased number and scope of investigations of fraud crimes would affect LEAs.
	Simplification benefits		Encouraging reporting could provide higher legal certainly, which would represent an improvement over the baseline.

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing		
Fundamental rights	► Personal data protection;	The exchange of information resulting from these provisions on encouraging reporting and information sharing would have to be carried out in full compliance with existing data protection rules.
	► Right to liberty and security	New provisions encouraging reporting and information sharing could have a positive effect on the right to liberty and security, as they are likely to enhance prevention.
	► Freedom to conduct business;	No significant impact.
	► Consumer protection	This measure indirectly improves consumer protection by enhancing information sharing.
	► Right to an effective remedy, in particular the remedies available before the courts.	No significant impact.
EU added value		This measure could bring moderate added value, in particular in the Member States that may have already incorporated obligatory (or voluntary) reporting provisions

www.parlament.gv.at

A4.1.2. Qualitative assessment of the policy options

The qualitative assessment of the **policy options**, based on the above assessment of the retained policy measures, was the following:

Option O: baseline			
Assessment criteria		**Description of the impacts and affected groups**	**Score**
Coherence	Internal	Maintaining the baseline is unlikely to address neither of the two general objectives.	0
	External	Maintaining the baseline is unlikely to raise specific issues since the Framework Decision is already coherent with the main EU legislation dealing with non-cash payment fraud. At the same time, neither additional synergies nor mutual reinforcing effects can be expected.	+0,5
Effectiveness	Social impacts	Maintaining the baseline would have no impact on **LEAs' capacity to address criminal activity**. This is because their capacity is related to the level of reporting required which is likely to remain the same. The **chances of detecting, prosecuting and sanctioning criminals** would be unchanged. No impact is expected. Barriers such as inadequate provisions and discrepancies in addressing non-cash means of payment, new forms of fraud, discrepancies in provisions establishing competent jurisdiction and in rules on extradition are likely to remain in place. The **number of criminal acts and organised crime gains** would be likely to continue rising. Payment card fraud would continue to be considered as a low risk and highly profitable activity by criminals: trends of fraudulent transactions would remain unchanged and the number of such transactions would further increase. The stakeholders affected include individual consumers and private sector representatives. The level of **protection for victims** of non-cash payment fraud is likely to remain the same – no impact is expected. Deficiencies in ensuring a satisfying level of protection, lack of provisions to protect victims of identity theft and insufficient information for victims of fraud	-0.5

www.parlament.gv.at

Option O: baseline			
		crime would not be addressed. The level of **co-operation between public institutions and private sector** is likely to remain the same – no impact is expected: without additional incentive so far only a few public-private partnerships have been established. Looking at aggregated impacts: The increasing number of criminal acts and organized crime gains are likely to have moderate negative impact on **security**.	
	Economic Impacts	A steady increase in number and value of non-cash payment transactions –a proxy for **consumption and trade flows-** is likely to continue at the same incremental pace. The stakeholders affected include individual consumers and private sector representatives. **Consumer choice** may decrease because of higher **risks of being victims of fraud** due to increasing use of cards and increasing value of fraudulent card transactions. The liability shift from consumers to the payment industry is likely to temper effects on individual customers. The **costs for economic operators** could increase (rather than fall) due to the need for better protection needed against new forms of crime. Payment industries and economic operators (SMEs in particular) would bear the higher costs. The impact is likely to be negative. Looking at aggregated impacts: Non-cash payment transactions facilitate digital purchases of services and goods thus improving the **functioning of the digital market and competition,** but the growing level of fraud and its costs are likely to bring about a negative (and moderate) impact, which would	-1.5

www.parlament.gv.at

Option O: baseline			
		limit the benefits stemming from easier, faster and cheaper transactions.	
Efficiency	Financial and administrative costs	By maintaining the baseline in this area, the administrative burden would be largely unchanged.	0
	Simplification benefits	No significant impact.	0
Fundamental rights		As regards to the impact of this option on fundamental rights, it is likely that with the baseline scenario, the perception of security would remain largely the same. Particular attention should be paid to the right to the protection of personal data (Article 8 of the EU Charter), considering that identity theft is a criminal conduct that can be preparatory or supportive to non-cash payment fraud and it is increasing: personal data continues to be stolen and used for fraudulent transactions. This is likely to continue without EU action and bring about economic and social costs, as described above. Whereas the General Data Protection Regulation is likely to lead to enhanced security measures by companies (e.g. merchants, intermediaries), possibly making data breaches less likely, this is not expected to deter organised crime from continuing their activities in attempting to and succeeding in stealing payment credentials. Only additional criminal law instruments are likely to provide a substantive contribution. With no further EU action, the level of consumer protection (guaranteed by Article 38 of the EU Charter) is likely to remain the same. As noted above, there are no provisions in the Framework Decision ensuring a minimum level of protection for victims of non-cash payment fraud and a minimum level of penalties and sanctions for fraud criminals.	0
EU added value		No significant impact.	0

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
Assessment criteria		**Description of the impacts and affected groups**	**Score**
Coherence	Internal	Improving implementation and enforcement of the Framework Decision could address the general objective of enhancing security by decreasing the occurrence of non-cash payment fraud, even if new forms of crimes would not be addressed at EU level. A self-regulatory framework for public-private cooperation could address the objective of reinforcing the trust of economic operators in the digital single market, being more involved in detecting and contrasting non-cash payment fraud. It could also affect consumers' trust, but mostly indirectly. Taking into account that measures under this option would not be legally binding, the overall impact is likely to be positive, yet small.	+1
	External	Providing guidance on how to implement the Framework Decision in synergy with the **PSD2**, the **Directive on attacks against information systems**, the **NIS directive** and the **Directive on victims' rights,** could improve enforcement. Providing adequate training to the relevant authorities on cybercrime and on how to provide better access of victims to their rights would also improve the enforcement of the **Directive on attacks against information systems** and of the **Directive on victims' rights**. Facilitating a self-regulatory framework for public-private cooperation would be complementary with the EU legislation aiming to improve public-private cooperation, such as : – the **Directive on attacks against information systems** which also aims to raise the awareness of SMEs about threats and vulnerabilities to such attacks; – the **NIS Directive** which also envisages close cooperation between designated authorities and data protection authorities;	+1

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
		Taking into account that measures under this option would not be legally binding, the overall impact is likely to be positive, yet small.	
Effectiveness	Social impacts	Compared to the baseline, **LEAs' capacity to address criminal activity** could increase through training courses, guidance, tools and campaigns and their possible participation in new public-private partnerships along with other stakeholders and gaining access to (better) information and good practice. However, LEAs capacity of addressing and prosecuting new methods of fraud would still be limited. The expected impact is small. The stakeholders affected are LEAs, judicial and judicial cooperation representatives, and the legal practitioners. The **chances of detecting, prosecuting and sanctioning criminals** are also expected to increase through training and better cooperation between public and private sectors, although these would still be limited to current legal provisions. The expected impact is small but it represents an improvement compared to policy option O. The stakeholders mostly affected are LEAs, judicial and legal profession, individual customers, victims' associations, national bank federations, and economic operators. The **number of criminal acts and organised crime gains** related to non-cash payment fraud (especially the new forms) could be only marginally lower than in the baseline: small impact. The stakeholders affected are private sector representatives (economic operators) and individual customers.	+1

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
		The level of **protection for victims** of non-cash payment fraud compared to the baseline is likely to slightly improve, due to enforced detection, prosecution and sanctioning as well as improved assistance to victims through better cooperation among interested entities. The stakeholders affected are consumers and economic operators. The level of **cooperation between public institutions and private sector** is likely to improve thanks to the self-regulatory framework. The impact could be moderate/significant, depending on the take up. The stakeholders affected are LEAs, private sectors representatives, banking federations, victim associations, EU institutions and public-private partnerships. Looking at **aggregated impacts**: Improved cooperation between public and private sectors and improved capacity to address non-cash payment fraud, together with enforced prosecution could lead to **small improvements of security**. **Overall social impact of the option: small and positive**	
	Economic Impacts	Improved implementation and enforcement of the Framework Decision, PSD2 and e-money Directive **(measure 1)** could bring results similar to policy option O: moderate increase in **consumption and trade flows**. This is due to training, guidelines and communication campaigns to raise awareness of non-cash payment fraud and good practice in addressing it, which could positively affect consumers' trust. Additional limited positive effects in terms of awareness and business climate can arise from the	-1

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
		establishment of public-private partnerships facilitated by a self-regulatory framework for public-private cooperation. The stakeholders affected are **individual consumers and economic operators**. The **risk for consumers of being victims of fraud** could fall slightly due to the campaigns and reinforced investigations and prosecutions and better information sharing through public-private partnerships, with marginal improvements of consumer choice. However, the level of fraud is likely to continue to grow because many areas (including new methods of payment and new forms of crime) may remain unregulated at EU level. The impact would be basically the same as in option O. The stakeholders affected are **individual consumers**. Slightly more benefits in the form of **cost savings to economic operators** can be expected compared to policy option O, given that new public-private partnerships would include representatives from the private sector. As such, the position of economic operators could be better protected, possibly resulting in lower costs of protecting against fraud. The expected impact is moderate. The stakeholders affected are economic operators, in particular big companies as SMEs may be unrepresented in new public-private partnerships. Looking at **aggregated impacts**: The level of fraud and its cost for individual consumers and economic operators is likely to be somewhat compensated by increasing consumption and the **overall impact** on	

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
		functioning of the digital market and competition could be **small and negative**. **<u>Overall economic impact of the option: small and negative</u>**	
Efficiency	Financial and administrative costs	The administrative burden would be higher than in policy option O, but very limited given that the legal basis for prosecuting fraud cases would remain unchanged. The main costs would consist of: – one-off costs for interested public and private stakeholders to set up public-private partnerships agreements ; – continuous (though very limited) costs for these stakeholders to participate in these agreements; – continuous costs for EU: training courses or workshop events with country representatives and LEAs; public campaigns to increase awareness of current provisions and good practice; other activities to help LEAs develop IT tools and human resources. Given that Member States and stakeholders are not required to implement the measures of the option, it is not possible to assess to which extent these actions would be taken up. **<u>Overall impact: small and negative</u>**	-1
	Simplification benefits	The proposed option is unlikely to lead to a further harmonisation of different national approaches or developing a single procedure for all Member States in case of cross-border cases. However, information about these differences would be better available and shared.	-0,5

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)			
		On the other hand, self-regulatory frameworks may actually increase the lack of legal certainty around the issues covered by self-regulation, especially if interpretations among different public-private partnerships agreements at the national level differ. **<u>Overall impact: very small and negative</u>**	
Fundamental rights		As regards to the impact of this policy option on fundamental rights, only minor improvements in consumer protection (Article 38) can be expected due to slightly reinforced prosecution of non-cash payment fraud (measure 1), although the unchanged scope of the legislation limits the magnitude of this impact. Personal data would continue to be stolen and used for fraudulent non-cash payment transactions. This is likely to continue (measure 1, measure 2). Nevertheless, an slightly improved capacity of law enforcement authorities could contribute to conduct a better assessment of the criminal offence and to safeguard the principle of legality and proportionality in criminal matters. It could also bring a slight improvement of LEAs contribution to the application of victims' rights during criminal proceeding (rights when making a complaint, rights when requesting information about their case, right to be heard, right to review a decision not to prosecute, right to be protected in the context of restorative justice). Public-private partnerships would need to be set (measure 2) respecting the existing data protection rules.	0

www.parlament.gv.at

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation (measures 1+2)		
	Overall impact: basically no impact	
EU added value	Better sharing of information and good practice, guidance, training and communication campaigns could facilitate cooperation in cross-border cases, compared to the baseline scenario, and it is unlikely to be achieved at the same scale by Member States acting alone. However, the magnitude of this added value is likely to be limited (to the scope of current legislation). It is not clear how effective the COM communication would be in incentivising voluntary public-private partnerships agreements. In addition, given that a number of such agreements already exist, the added value of the communication is likely to be quite limited. Where the value could be still added is the governance of such agreements in terms of e.g. liability, management of shared information. **Overall impact: very small positive impact**	+0.5

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
Assessment criteria		**Description of the impacts and affected groups**	**Score**
Coherence	Internal	As compared to policy option A, this option can better responds to both general objectives: – firstly, broad minimum common definitions (measure 3) and minimum sanctions (measure 5) would address different forms of fraud, including new and emerging ones, cross-border crimes (measure 12 and measure 7), and preparatory activities (measure 5); – secondly, by addressing these types of fraud and conduct, this option would raise consumers' and economic operators' trust in non-cash payment transactions and the digital single market. **Overall impact: moderate and positive**	+2
	External	This option would be consistent with the definition of payment instrument (measure 3) of the PSD2 and with the Regulation on interchange fees for card-based payment transactions, which uses the same definition. This option is consistent with Directive 2013/40/EU on attacks against information systems, by using it as a reference for defining jurisdiction rules (measure 7). The option would also complement the minimum rules established by the Directive on Euro counterfeiting that defines criminal offences and sanctions and sets up minimum maximum levels of penalties for counterfeiting of physical currencies. Collecting statistics on investigations and prosecutions at EU level (measure 12) is consistent with Regulation No 223/2009 on European statistics Eurostat and with the fourth AML Directive. Strengthening the role of the contact point would support the application of both of Regulation (EU) 2016/794 on Europol and of Council Decision 2009/426/JHA on the strengthening of Eurojust.	+2

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
		<u>Overall impact: moderate and positive</u>	
Effectiveness	Social impacts	This option would have an impact **LEAs capacity to address a wider spectrum of criminal activities** (measure 3) and preparatory activities (measure 5). It could also strengthen the role of national contact points (measure 12). The implementation of this option would require LEAs to have an adequate level of resources for investigating and persecuting the new forms of crimes (measure 3 and measure 5), as well as for collecting stats on investigations and prosecutions (measure 12). As a whole, the impact on LEAs capacity could be small in the short term, but it could increase over time if resources are made available. The **chances of detecting, prosecuting and sanctioning criminals** could increase through: a) the broad definition of non-cash payment transactions and fraud crimes, covering new and emerging forms of crimes (measure 3); b) **criminalisation of preparatory acts** and common minimum levels of maximum sanctions (measure 5); c) facilitating LEAs cooperation and exchange of information (measure 12), especially through updated jurisdiction rules (measure 7). The impact could be significant and positive, with an improvement if compared to policy option O. The stakeholders affected include LEAs, judicial representatives and legal practitioners. Criminalising preparatory/supportive conduct and setting minimum levels of maximum sanctions for both non-cash payment fraud and preparatory/supportive conduct (measure 5) could have a deterrent effect, thus preventing and limiting the **number of fraud and organised crime gains**. In general, the impact is likely to be positive and moderate compared to option O,	+2

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
		The stakeholders affected include individual consumers and economic operators. The impact on the level of **protection for victims** is likely to be moderate. This is because the new EU definitions (measure 3) would provide protection from a wider range of new and future fraud crimes, while criminalisation of preparatory activities (measure 5) would expand protection to potential victims and the measures addressing obstacles to cooperation due to legal and operational reasons (measure 7 and measure 12) would enhance protection of victims of complex cross-border fraud cases. However, the option does not foresee any measure addressing the actual rights of the victims (direct approach)[148]. Improved assistance to victims could therefore only be expected through better cooperation among interested entities participating in public-private partnerships (measure 2). The stakeholders affected include individual consumers and economic operators. Likewise, the **level of cooperation between public institutions and the private sector** is likely to improve because of the self-regulatory framework (measure 2). The impact could be moderate/significant, depending on the take up. Looking at **aggregated impacts**:	

[148] Direct approach refers to the adoption of specific provisions regarding victims' rights which are complementary to those provided by Directive 2012/29/EU.

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
		A positive **impact** could be expected in terms of the **improvement of security,** mostly due to the increased chances of detecting, prosecuting and sanctioning criminals**.** However, given the lack of binding measures addressing the rights of non-cash payment fraud' victims and the cooperation between public and private sectors, the impact is likely to be moderate. **<u>Overall economic impact of the option: moderate and positive</u>**	
	Economic Impacts	Same as policy option A with regard to measure 2. Only additional impacts are described. A broad and technology-neutral definition of non-cash payment instruments and related crimes (measure 3) would extend the coverage of EU legislation especially around new payment instruments, while setting a minimum level of maximum sanctions for fraudulent activities and for actions preparatory to and supportive of fraud (measure 5) could better prevent fraud. Updated jurisdiction rules (measure 7) and improved cooperation between Member States (measure 12) could also help to better tackle cross-border crimes. As a result, the enhanced protection of customers could help build trust on the security of non-cash payment transactions, leading to increased **consumption and trade flows** in the medium and long term. The increase would be higher than in the baseline: moderate positive impact. The stakeholders affected include individual consumers and economic operators. Preparatory actions could be prosecuted and sanctioned regardless of whether the fraud actually occurred (measure 5). This would be complemented with addressing new forms of non-cash payments and crimes (measure 3), clarifying the rules on jurisdiction (measure 7), incentivising	+2

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
		sharing of information among Member States and strengthening the role of dedicated national contact points (measure 12). As a result, improvements in the level of **risk of being victims of fraud** and thus **consumer choice** could be significant, compared to policy option O. The stakeholders affected include individual consumers. A moderate impact is expected in terms of **cost savings for economic operators**. If resourced appropriately, enforcement agencies would be able to step in sooner (**measure 5)** and more effectively for a wider range of cases (**measure 3** and **measure 5),** including cross-border ones (**measure 12 and measure 7).** As a result, potential financial losses could be prevented or at least limited to a higher extent than in option O. The stakeholders affected include economic operators; in particular big companies, such as card issuers that bear most of the costs. However, the benefits are likely to spill over to other firms, including SMEs, as the cost of doing business could be reduced. Looking at **aggregated impacts**: Accumulated benefits of consumptions, trade flows, consumer choice and cost savings for economic operators could generate a **positive impact on the digital single market,** mitigated by the increased administrative and financial costs (see Efficiency below) related to this option. **Overall economic impact of the option: moderate/significant and positive**	

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
Efficiency	Financial and administrative costs	Compared to policy option O, this option could increase the administrative burden for the EU institutions and Member States. The following costs are expected: – one-off costs for the EU: developing new legislation (e.g. definition of non-cash payment instruments based on PSD2 definition, crimes and preparatory conduct) and minimum level of maximum sanctions; – one-off costs for Member States: adopting new provisions in their national settings (e.g.: as the legislation would only set a minimum level of sanctions for the maximum penalty, it would leave flexibility as to setting the ceilings, as well as levels for the minimum penalty; these, if defined in national legislation would have to be adjusted); – continuous costs for EU : facilitating cooperation through Eurojust among all Member States claiming jurisdiction over the same case (measure 7) – continuous costs for Member States: implementing and enforcing the new legislation, such as costs for investigating and persecuting the crimes under the scope of the option (measure 3 and measure 5), costs for collecting stats on investigations and prosecutions, and sharing them with other Member States (measure 12) ; costs for cooperating with other Member States concerned by the same cross-border cases (measure 7) Overall, the cumulative impact of this option on administrative and financial costs could be very high for those Member States that would face a significant increase of possible crimes because of the new definitions and the criminalisation of preparatory conduct, not currently covered by their national legislation.[149] Therefore, the administrative and financial impacts could be at least moderate, primarily affecting LEAs, judiciary, legal practitioners and EU institutions.	-1.5

[149] As regards to preparatory activities, available data suggest that there are few Member States that do not criminalise several activities (such as social engineering, data breaches, identity theft and acting as a money mule).

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)			
		Overall impact: moderate and negative	
	Simplification benefits	This option would further approximate the national criminal law frameworks, providing common definitions (measure 3) and a common minimum level of sanctions for the maximum penalty (measure 5). Reducing the differences between Member States should also facilitate the cooperation between Member States in investigating and prosecuting cross-border cases. To this end, the updated rules on jurisdiction (measure 7), the reinforced role of national contact points and the exchange of information between Member States (measure 12) could further simplify the procedures and practices for cooperating. However, broad and all-encompassing definitions: – could be more difficult to transpose to national legislation in Member States where a detailed definition was adopted (e.g. DE); – could be open to diverse interpretations, limiting the simplification benefits. **Overall impact: small and positive**	+1
Fundamental rights		The option would have a positive impact on **the right to security** (Article 6 of the EU Charter) and **consumer protection** (Article 38 of the EU Charter) by regulating forms of non-cash payment not covered by current EU legislation, improving chances of prosecuting fraudsters, and better protecting victims of non-cash payment fraud and associated preparatory conduct (measures 3 and 5). In addition, **consumer protection** is likely to be improved by:	+1.5

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)		
	- better information sharing (measure 12) - updating rules on jurisdiction, possibly making it easier to pursue complex cross-border fraud cases (measure 7). The criminalisation of some preparatory activities (such as stealing of data, trafficking of credentials, identity theft - measure 5) would indirectly contribute to **protection of personal data** (Article 8 of the EU Charter) compared to the baseline scenario. The establishment of public-private partnerships (measure 2) should be done in coherence with the existing data protection rules, in particular with regard to the sharing and processing of personal data. **Overall impact: moderate and positive.**	
EU added value	Although representing a significant improvement to the Framework Decision, the new EU definitions of non-cash payment instruments and offences (including preparatory activities) could have a moderate added value in the Member States that may have already adopted the PSD2 definition and/or may have already criminalised new forms of crime and preparatory conduct in their national legislation. However, a higher EU added value can be associated to the provision setting minimum levels of sanctions (which could reduce the disparities between Member States and to ensure a more coherent treatment of fraud criminals across EU), as well as to those provisions facilitating cross-border cooperation. Member States would be unlikely to effective ensure cross border investigation and prosecution of non-cash payment fraud without EU action.	+1.5

www.parlament.gv.at

Option B: introduce a new legislative framework and facilitate self-regulation for public-private cooperation (measures 2+3+5+7+12)		
	Overall impact: moderate and positive	

www.parlament.gv.at

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
Assessment criteria		**Description of the impacts and affected groups**	**Score**
Coherence	Internal (Relevance)	*Same as policy option B with regard to **measures 3, 5, 7 and 12**. Only additional intermediate impacts are described, while aggregate and overall impacts are presented for the option as a whole, in each of the assessment criteria.* This option would better pursue the general objective of reinforcing the trust of consumers and economic operators, through specific protection to natural and legal persons (measure 11). **Overall impact: significant and positive**	+2.5
	External	This option would provide protection also for legal persons who are victims of non-cash payment crimes (measure 11), complementing the **Directive on victims' rights** that defines as victim only a natural person. This option could also complement the **PSD2** which sets provisions payment service providers on the reporting of incidents relating to the unauthorised or fraudulent use of the payment instrument (measure 14). **Overall impact: moderate and positive**	+2

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
Effectiveness	Social impacts	**LEAs' capacity to address criminal activity** could be improved through the cooperation with the private sector thanks to the establishment of public-private partnerships and encouraging reporting (measure 14). These could enable the sharing of strategic information (such as most significant fraud incidents and/or suspicious transactions, new threats and modi operandi), expertise and good practices. The expected impact would range from small to significant, depending on the extent to which partners' liabilities and responsibilities would be addressed within the public-private partnerships and the frequency and nature of reported information. The legal certainty of reporting and setting up of dedicated channels and tools for facilitating it (measure 14) could increase the **chances of detecting, prosecuting and sanctioning perpetrators.** Furthermore, encouraging reporting could help LEAs to get targeted information and focus on major perpetrators. The expected impact would range from small to significant (+1/+2.5), depending on the frequency and nature of information actually reported by the private sector. The stakeholders mostly affected are LEAs, economic operators, National Banking Federations, and individual consumers. This option could improve the **protection for victims,** granting additional specific rights (measure 11) to both natural and legal persons to reduce the negative consequences of both new forms fraud (measure 3) and preparatory activities (measure	+2.5

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
		5). Specifically, the option would address the non-financial costs (such as those attached to identity theft)[150] borne by the victims, including citizens and SMEs.[151] Further protection for legal persons could arise from provisions encouraging reporting. The expected impact could be significant and positive. The stakeholders affected are individual consumers and economic operators, especially SMEs. The level of **cooperation between public institutions and private sector** could increase through the establishment of public-private partnerships and other provisions consistent with the principle of cooperation, such as encouraging reporting (measure 14). The expected impact could range from small to significant, depending on the extent to which partners' liabilities and responsibilities would be addressed within the public-private partnerships. Looking at **aggregated impacts**: A **significant impact** is expected in terms of the **improvement of security,** due to the increased chances of detecting, prosecuting and sanctioning criminals (measure 3, measure 5, measure 12 and measure 7), the enhanced protection of non-cash payment	

[150] Examples of such costs are: reputational damage, psychological and social distress, impacts on fundamental rights (e.g. data protection and privacy) and costs to rectify the consequences of the theft (e.g. replacing identity documents).
[151] Legal persons can suffer of reputational damage. For instance, in 2011 Sony's PlayStation Network was victim of cyberattack stealing credit card credentials of an estimated 77 million people, which also damaged the reputation of the company. SMEs can be more vulnerable than larger companies to the negative consequences of identity theft. .

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
		fraud' victims (measure 11) and the facilitation of public-private cooperation and of reporting (measure 14). **<u>Overall economic impact of the option: significant and positive</u>**	
	Economic Impacts	The option foresees provisions to protect natural and legal persons (**measure 11)** that could further build trust in non-cash payment transactions, reduce the financial and social costs attached to fraud (especially identity theft) and increase business-to-business online transactions, especially involving SMEs. This could lead to increased **consumption and trade flows** compared with both the baseline and policy option B. The stakeholders affected are individual consumers and economic operators, including SMEs. Stronger public-private cooperation (measure 14) could enable the exchange of strategic information (e.g. about new threats/modi operandi), which could improve prevention, reduce the **risk of being victim of fraud** and improve **consumer choice** in a moderate manner. The protection for legal persons (measure 11) could bring **cost savings to companies** and in particular SMEs, which are likely to be more vulnerable to fraud and their negative financial effects. Furthermore, economic operators would be encouraged to report. In the case of voluntary reporting, they would likely report only the most significant non-cash payment fraud and incidents (that are likely to lead to significant financial losses to them if not contrasted), while not bearing additional costs due to mandatory reporting (measure 14). The impact could be moderate. The stakeholders	+2.5

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
		affected are economic operators, including SMEs. Looking at **aggregated impacts**: Accumulated benefits (measure 3, measure 5, measure 12, measure 7, measure 14, measure 11) of consumer choice and protection (both natural and legal persons), consumptions (both business-to-customer and business-to-business), and cost savings for economic operators could drive **significant positive impacts on functioning of the digital market and competition,** mitigated by the increased administrative and financial costs (see Efficiency below). **Overall economic impact of the option: significant and positive**	
Efficiency	Financial and administrative costs	This option could increase the administrative burden for the EU institutions and Member States. The most likely additional costs associated with this option include: – one-off costs for the Member States for setting-up public-private partnerships, as well as dedicated channels and tools for facilitating reporting (measure 14); – continuous costs for Member States: implementing a wider protection for natural and legal persons; education measures, communication campaigns (measure 11), support the running the established public-private partnerships (measure 14). – continuous costs for LEAs: maintaining dedicated channels and tools to facilitate reporting (measure 14). continuous costs for economic operators: reporting targeted non-cash payment fraud cases (measure 14).	-2

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)			
		Additional costs would mostly affect LEAs**,** without imposing any significant cost to the private sector and citizens due to the non-mandatory nature of reporting. **Overall impact: moderate and negative**	
	Simplification benefits	This option could bring some additional simplification benefits, since the legal certainty for reporting and the establishment of specific channels and tools for facilitating it (measure 14), as well as the lack of additional administrative burden on the private sector and citizens. **Overall impact: moderate and positive**	+1.5
Fundamental rights		This option could improve **consumer protection** (Article 38 of the EU Charter) for natural and legal persons which are victims of non-cash payment crimes (including identity theft), through assistance and support services, awareness campaigns and other provisions addressing the negative financial and non-financial consequences (measures 10 and 11). At the same time, information gathering and sharing required to fight crime (measure 14) can also affect the privacy and **data protection** rights (Article 8) of the victims or third parties where their personal data are concerned and so it is important to provide adequate safeguards in this field by ensuring full compliance with EU data protection rules. A particular attention should be paid to the protection of the victims' rights when participating in criminal proceedings (Chapter 3 of Directive 2012/29/EU), respectively to the assurance of a fair trial (Art. 47 of the EU Charter) both in home and foreign jurisdictions. Moreover, it is important that the transfer of personal data should	+2

www.parlament.gv.at

Option C: same as option B but with provisions on encouraging reporting for public-private cooperation instead of on self-regulation, and new provisions on raising awareness (measures 3+5+7+11+12+14)		
	not go beyond the purpose for which data is used, in order to comply with the rights of protection the privacy, personal integrity and personal data of the victim. **Overall impact: moderate and positive**	
EU added value	It is unlikely that Member States would be able to achieve a similar level of approximation in protection for both natural and legal persons without EU action (measure 11). Specifically, although a number of Member States already cover identity theft in their national legislation, the rights of the victims are included in the same general guarantees for the fraud attacks, without specific protection against the negative consequences of it (such as rectification of negative entries in victims' credit history). **Overall impact: significant and positive**	+2.5

www.parlament.gv.at

Option D: same as option C but with additional jurisdiction provisions complementing EIO and injunction rules (measures 3+5+7+8+9+11+12+14)			
Assessment criteria		**Description of the impacts and affected groups**	**Score**
Coherence	Internal	*Same as policy option C with regard to **measures 3, 5, 7, 11, 12 and 14.** Only additional specific impacts are described, while overall impact is presented for the option as a whole, in each of the assessment criteria.* This option would likely reinforce investigations and prosecutions through the additional measures 8 and 9 in relation option C, which are likely to further enhance security and reinforce consumers' trust.	+3
	External	This option has the same consistencies with the EU and international legal framework than policy option C except that this option would regulate the access to the electronic evidence when the Commission is currently developing an horizontal initiative to address this issue in a horizontal way and not only for non-cash payment fraud offences (measure 9). Also, this option includes provisions to complement the European Investigation Order (measure 8), with which they would be coherent.	-2
Effectiveness	Social impacts	This option could increase the chances for detecting, prosecuting and sanctioning offenders, by building on currently existing law enforcement mechanisms for cross-border cooperation, such as the EIO (measure 8) and the injunctions (measure 9) for cooperation. The level of protection for victims could increase slightly compared to option C thanks to improved cross-border investigation and prosecution (measure 9).	+3

www.parlament.gv.at

Option D: same as option C but with additional jurisdiction provisions complementing EIO and injunction rules (measures 3+5+7+8+9+11+12+14)			
		<u>Overall impact: significant and positive</u> Looking at aggregated impacts: Enhanced investigation and prosecution of criminals and protection for victims could contribute to the improvement of security. The impact is likely to be significant and positive.	
	Economic Impacts	In this option the consumption and trade flows could increase thanks to reinforced law enforcement (measure 8) and judicial (measure 9) cooperation, which could help decrease the level of fraud. This could bring significant and positive impact. **<u>Overall impact: significant and positive</u>** Looking at aggregated impacts: Increasing level of consumption and trade flows could contribute to better functioning of the digital single market, and have a positive economic impact, mitigated by financial and administrative costs.	+3
Efficiency	Financial and administrative costs	Complementing the EIO (measure 8) and maintaining a database in injunctions (measure 9) in order to better monitor injunction orders, could entail additional continuous costs for	-3

www.parlament.gv.at

Option D: same as option C but with additional jurisdiction provisions complementing EIO and injunction rules (measures 3+5+7+8+9+11+12+14)			
		Member States, such as processing the increased number of EIO requests and provide feedback to the executing authority. The increased number and scope of investigations of fraud crimes would mainly affect LEAs, judiciary, legal practitioners. **Overall impact: significant and negative**	
	Simplification benefits	This option could have the same simplification benefits as option C. In addition, the complemented EIO (measure 8) and injunctions (measure 9) could further improve the efficiency of existing mechanisms for cross-border cooperation, resulting in small, additional simplification benefits. **Overall impact: moderate and positive**	+1
Fundamental rights		Accessing evidence across borders could help effective detection and prosecution of crimes, and the protection of victims of crime. At the same time, measures to facilitate cross-border access to evidence, may raise questions of impact on fundamental rights. Any legislative initiative must respect the right to fair trial and include safeguards to protect the rights of the persons affected, including the rights of the defence, the right to an effective remedy as well as other procedural rights. Another important aspect is the impact on the fundamental rights to data protection and privacy. Respect of data protection rules is paramount both for law enforcement when sending requests and for the addressees of those requests, when responding to them. At the same time, this option could also strengthen consumer protection (Article 38)	2

www.parlament.gv.at

Option D: same as option C but with additional jurisdiction provisions complementing EIO and injunction rules (measures 3+5+7+8+9+11+12+14)		
	against fraud while respecting victims' privacy at the same time (measure 9). **<u>Overall impact: moderate and positive</u>**	
EU added value	This option could have additional EU value compared to option C, by further reinforcing cross-border investigation and prosecution. **<u>Overall impact: significant and positive</u>**	+3

www.parlament.gv.at

A4.2. Quantitative assessment

A4.2.1. Quantitative assessment of the policy measures

Table 1 below describes the quantitative assessment of the costs for the retained policy measures:

Table 1: estimation of one-off and continuous (annual) costs for each retained policy measure (EUR)

0: Baseline						
One-off and continuous	Description					
	With no EU action in this area the administration burden could remain unchanged					
	Total one-off and continuous	**0**				
1: Improve implementation						
One-off	Description	Days * daily rate	Work days	A8 daily rate		
	EU: publication of the 3rd implementation report	€ 9,000	30	€ 300		
	EU: publication of a guidebook on national legislations to foster cooperation	€ 9,000	30	€ 300		
	Total one-off	**€ 18,000**				
Continuous	Description	Days * daily rate	Work days	A8 daily rate		
	EU: training courses or workshop events with country representatives and LEAs;	€ 8,400	28	€ 300		
	EU: other activities to help LEAs develop IT tools and human resources.	€ 8,400	28	€ 300		
	EU: additional costs to promote the exchange of best practices	€ 120,000				
	Total continuous	**€ 136,800**				

www.parlament.gv.at

2: Include self-regulatory framework						
One-off	Description	Days * daily rate	Work days	A8 daily rate		
	EU: develop and publish the communication	€ 18,000	60	€ 300		
	EU/MS: costs for interested stakeholders to set up public-private partnerships agreements (negligible)	€ 0				
	Total one-off	**€ 18,000**				
Continuous	EU/MS: continuous (though very limited) costs for stakeholders to participate in public-private partnerships agreements	0				
	Total continuous	**0**				
3: Include technology neutral definitions						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing a new definition (drawing on and potentially expanding the PSD2 definition)	€ 18,000	60	€ 300		
		Total MS	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adopting this new definition in their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total MS	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: implementing a wider substantive scope of the Framework Decision	€ 526,500	27	€ 19,500	150	€ 130
	Total continuous	**€ 526,500**				

www.parlament.gv.at

5: Criminalise preparatory acts as a separate offence and set minimum levels of maximum penalties for all offences						
One-off	Description	Days * daily rate	Work days	A8 daily rate		
	EU: developing a new legislation	€ 24,000	80	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adopting new provisions to their national settings (as the legislation would only set a minimum level of sanctions for the maximum penalty, it would leave flexibility as to setting the ceilings, as well as levels for the minimum penalty - these, if defined in national legislation would have to be adjusted)	€ 210,600	27	€ 7,800	60	€ 130
	Total one-off	**€ 234,600**				
Continuous	Description	Total MS	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: implementing the new legislation	€ 351,000	27	€ 13,000	100	€ 130
	MS: increased number of cases for investigation as a result of the new legislation	€ 338,000	13	€ 26,000	200	€ 130
	Total continuous	**€ 689,000**				

www.parlament.gv.at

7: Update jurisdiction rules in line with those in AAIS Directive						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing the new legislation	€ 18,000	60	€ 300		
	Description	Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adopting new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	Work days	A8 daily rate		
	EU: facilitating cooperation among all affected Member States through Eurojust	€ 3,600	12	€ 300		
			Nr of Member States affected	Total per MS	Work days	Civil servant daily wage
	MS: cooperation with all affected MS	€ 42,120	27	€ 1,560	12	€ 130
			MS affected	Total per MS	Work days	Civil servant daily wage
	MS: centralising proceedings in a single Member States (for each proceeding only one Member States would have to follow up with an investigation); and cybercrime cases that include non-cash payment fraud and a foreign element are limited.	€ 2,600	1	€ 2,600	20	€ 130
	Total continuous costs MS	€ 44,720				
	Total continuous	**€ 48,320**				

www.parlament.gv.at

8: Extend jurisdiction rules to complement the European Investigation Order						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing a new legislation	€ 18,000	60	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adopting new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: implementation costs	€ 351,000	27	€ 13,000	100	€ 130
	Total continuous	**€ 351,000**				
9: Adapt rules on injunction for cooperation/evidence purposes						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing new legislation	€ 18,000	60	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adapting the new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: implementation costs	€ 351,000	27	€ 13,000	100	€ 130
	Total continuous	**€ 351,000**				

www.parlament.gv.at

11: Add provisions protecting natural and legal persons from identity theft						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing new legislation	€ 18,000	60	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adapting the new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: implementing a wider protection for natural and legal persons	€ 351,000	27	€ 13,000	100	€ 130
	MS: education measures, awareness raising campaigns	€ 351,000	27	€ 13,000	100	€ 130
	Total continuous	**€ 702,000**				

12: Facilitate cross-border cooperation						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing new legislation	€ 18,000	60	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adapting the new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	Work days	A8 daily rate		
	EU: incentivising Member States to share information with Europol	€ 3,600	12	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: collecting stats on investigations and prosecutions of non-cash payment fraud	€ 42,120	27	€ 1,560	12	€ 130
	MS: designating & maintaining several (5) contact points x 12 days = 60	€ 210,600	27	€ 7,800	60	€ 130
	Total continuous costs MS	€ 252,720				
	Total continuous	**€ 256,320**				

www.parlament.gv.at

14: Encourage reporting to law enforcement and information sharing						
One-off	Description	Days * rate	Work days	A8 daily rate		
	EU: developing new legislation	€ 18,000	60	€ 300		
		Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: adapting the new provisions to their national settings	€ 70,200	27	€ 2,600	20	€ 130
	Total one-off	**€ 88,200**				
Continuous	Description	Total	MS affected	Total per MS	Work days	Civil servant daily wage
	MS: costs for LEAs for creating and maintaining dedicated points of contact to facilitate cross-border cooperation	€ 70,200	27	€ 2,600	20	€ 130
	Total continuous	**€ 70,200**				

www.parlament.gv.at

Table 2: summary of one-off and continuous (annual) costs for each retained policy measure (EUR)

	ONE-OFF COSTS			CONTINUOUS (ANNUAL) COSTS		
POLICY MEASURES	EU	MEMBER STATES	TOTAL EU+MS	EU	MEMBER STATES	TOTAL EU+MS
1	€ 18,000	€ 0	€ 18,000	€ 136,800	€ 0	€ 136,800
2	€ 18,000	€ 0	€ 18,000	€ 0	€ 0	€ 0
3	€ 18,000	€ 70,200	€ 88,200	€ 0	€ 526,500	€ 526,500
5	€ 24,000	€ 210,600	€ 234,600	€ 0	€ 689,000	€ 689,000
7	€ 18,000	€ 70,200	€ 88,200	€ 3,600	€ 44,720	€ 48,320
8	€ 18,000	€ 70,200	€ 88,200	€ 0	€ 351,000	€ 351,000
9	€ 18,000	€ 70,200	€ 88,200	€ 0	€ 351,000	€ 351,000
11	€ 18,000	€ 70,200	€ 88,200	€ 0	€ 702,000	€ 702,000
12	€ 18,000	€ 70,200	€ 88,200	€ 3,600	€ 252,720	€ 256,320
14	€ 18,000	€ 70,200	€ 88,200	€ 0	€ 70,200	€ 70,200

www.parlament.gv.at

A4.2.2. Quantitative assessment of the policy options

Table 3 below describes the quantitative assessment of the costs for the policy options, based on the above quantitative assessment of the retained policy measures:

Table 3: summary of one-off and continuous (annual) costs for each policy option (EUR)

	ONE-OFF COSTS			**CONTINUOUS (ANNUAL) COSTS**		
POLICY OPTIONS	EU	MEMBER STATES	TOTAL EU+MS	EU	MEMBER STATES	TOTAL EU+MS
O	€ 0	€ 0	€ 0	€ 0	€ 0	€ 0
A (measures 1+2)	€ 36,000	€ 0	€ 36,000	€ 136,800	€ 0	€ 136,800
B (2+3+5+7+12)	€ 96,000	€ 421,200	€ 517,200	€ 7,200	€ 1,512,940	€ 1,520,140
C (3+5+7+11+12+14)	€ 114,000	€ 561,600	€ 675,600	€ 7,200	€ 2,285,140	€ 2,292,340
D (3+5+7+8+9+11+12+14)	€ 150,000	€ 702,000	€ 852,000	€ 7,200	€ 2,987,140	€ 2,994,340

www.parlament.gv.at

ANNEX 5: EVALUATION OF THE EXISTING POLICY AND LEGISLATIVE FRAMEWORK

1. Executive summary

The **Council Framework Decision 2001/413/JHA** (hereinafter also referred to as 'the Framework Decision') on combating fraud and counterfeiting of non-cash means of payment has been applicable since 2 June 2003. The Framework Decision aims to harmonise the scope of what should be considered a criminal offence, make sure that Member States take action to sanction these offences and foster cross-border cooperation and exchange of information.

The evaluation performed aimed at understanding to what extent the Framework Decision has achieved its original objectives in terms of relevance, effectiveness, efficiency, coherence, and EU added value. It also analysed the practical implementation of the Framework Decision in Member States. Finally it evaluated the current situation in areas related but not included in the scope of the Framework Decision, such as reporting, public-private cooperation and victims' rights.

Relevance

The scope of the Framework Decision is not fully relevant in view of recent technological developments. The definition of payment instruments included in the Framework Decision does not cover those that are emerging, namely non-corporeal means of payment (such as virtual payment cards, mobile money, virtual currencies) that are increasingly targeted by fraudsters. The Framework Decision definition is partially outdated as it covers means of payment that are no longer issued, such as 'eurocheque cards' or 'eurocheques'. As further evidence of the limited relevance of the Framework Decision definition, it is worth highlighting the fact that most of the Member States adopted wider, and therefore more stringent, definitions of payment instruments.

As for criminal offences, the types of conduct to be criminalised according to the Framework Decision still reflect the components of non-cash payment (non-cash payment) fraud. However, there are some behaviours, currently out of the scope of the Framework Decision, which are gaining importance, such as social engineering and carding websites. The Framework Decision appears to be only partially relevant in so far as it limits the scope of some punishable forms of conduct (Art. 2) when relating to corporeal instruments. Moreover, it does not cover conduct that is preparatory and supportive (e.g. identity theft) to offences related to computers (Art.3) without resulting directly in a transfer of money or monetary value. The fact that many Member States went beyond the Framework Decision and developed provisions to cover additional trends in terms of non-cash payment fraud is additional evidence of the limited relevance of the Framework Decision in this regard.

Effectiveness

The Framework Decision has only partially met its strategic objective of creating conditions for effective investigations and prosecutions. Its main contributions to the current situation are the approximation of national legislation (there is evidence of a low level of harmonisation of national law before the implementation of the Framework Decision), and

www.parlament.gv.at

the provision of principles and high level guidelines to investigations, prosecutions, and cross-border cooperation.

However, there are operational shortcomings in the activities of law enforcement agencies and judicial representatives, which may limit the benefits of the current approximation of national laws. Investigations and prosecutions are also hindered by obstacles in cooperation mechanisms between Member States and practices for information exchange.

The current conditions for investigations and prosecutions are also the result of positive parallel topics that are not explicitly covered by the Framework Decision.

1. Firstly, most Member States adopted provisions in their national legislation or ad-hoc mechanisms to favour reporting practices and/or make it mandatory under national legislation to report to law enforcement authorities whenever there are suspicions raised. Notwithstanding, underreporting remains quite common in non-cash payment fraud.
2. Secondly, there is evidence of a limited number of initiatives in the field of public-private cooperation at both EU and national level which contributed to a better exchange of information in investigations and prosecutions. This type of cooperation is often driven by the need of public authorities to obtain information to be used as evidence, in prevention and detection of non-cash payment fraud. However, such initiatives are hampered by the existence of different national data protection laws, and the lack of clarity in the rules to be followed by private stakeholders.
3. Finally, the coverage of rights ensured by the current legislative framework appears to be not fully adequate to the needs of victims of fraud and/or identity theft. Besides the lack of harmonisation of national legislative frameworks, limited satisfaction is also linked to their poor enforcement. Even though a number of initiatives already exist at national level, the level of protection should increase with the implementation of the Victims' Directive[152] by the end of November 2017. The need to be assisted, the need to access information and support services, and the need to recover losses have been identified as insufficiently met. Furthermore, there is a lack of provisions, at both EU and at national level, addressing explicitly the victims of identity theft. In addition the Victims' Directive covers only natural persons, not legal ones.

Efficiency

The cost of non-cash payment fraud is over €1.44 billion for the EU and is likely to increase. Payment services providers (in particular financial institutions and card issuers) bear most of the costs relating to fraudulent transactions. Payment card fraud is a highly profitable activity for organized crime groups. Europol reported in 2012 that their revenues in this field originating from the EU were around €1.5 billion per year. The airline sector seems to be among the most affected industries.

[152]Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012establishing minimum standards on the rights, support and protection of victims of crime.

Coherence

The Framework Decision is coherent with the main EU and international legislation dealing with non-cash payment fraud and counterfeiting, notably with the Revised Payment Services Directive[153] and Directive on Attacks Against Information Systems[154]. In most cases, EU and international legislation partially integrate the Framework Decision provisions by making the overall criminal law framework more relevant to recent technological developments.

EU added value

The Framework Decision added value by setting a common criminal law framework of reference for Member States, even though this is also the result of the co-existence of other relevant EU legislation.

2. Introduction

Purpose

The present report evaluates the existing policy and legislative framework (and namely the legislative measures transposing the Council Framework Decision 2001/413/JHA- hereafter the Framework Decision) in combatting fraud and counterfeiting of non-cash means of payment, against the background of the broader EU and international context.

It includes:

- a brief description of the Framework Decision and its different components, its objectives and the problems it was intended to solve (its intervention logic)
- an assessment of the level of implementation of the Framework Decision in the national laws
- an evaluation of the effectiveness, efficiency, relevance, coherence and EU added value of the Framework Decision
- preliminary identification of areas where a possible EU intervention is needed to better tackle non-cash payment fraud, in terms of reaction and prevention.

The report does not include a detailed analysis of the non-cash payment industry and of the dimension of related crimes, as those are part of the main Impact Assessment report, to which this report is annexed.

[153] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015on payment services in the internal market.
[154] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013on attacks against information systems.

www.parlament.gv.at

As described in annex 1 (section 3 on evidence), given that evidence was already available on difficulties encountered by law enforcement in tackling non-cash payment fraud, the decision was taken to run the evaluation of the current situation at the same time with the impact assessment.

The report constitutes the basis for assessing the need for further EU intervention aiming at combating fraud and counterfeiting of non-cash means of payment.

Scope of the report

- Content:
  - The Council Framework Decision 2001/413/JHA
  - National legislation (laws, regulations and administrative procedures and protocols of general applicability) transposing the Framework Decision and addressing fraud and counterfeiting of non-cash means of payment;
  - Case law of the European Court of Justice and of national courts;
  - Relevant EU and international legislative and policy context;
  - Areas not included in the scope of the Framework Decision, which are relevant to achieve its objective and address the problems it is supposed to solve

  - The report covers the following key areas of analysis:
    - The *criminal law framework* including national laws transposing the Framework Decision, and key European and international legislation regarding non-cash means of payment fraud and counterfeiting.
    - *Procedural criminal law,* including obstacles to investigations and prosecutions and conditions for good law enforcement and judicial cooperation.
    - *Conditions for reporting and public-private cooperation* covering reporting obligations, practices of cooperation between law enforcement, judiciary, financial institutions and payment service providers, and bottlenecks and enablers to cooperation.
    - *Victims' rights* with a focus on the main consequences for individuals that are victims of fraud and/or identity theft and the current level of protection ensured to victims by EU and national legislation.[155]
  - The evaluation is undertaken against **five mandatory evaluation criteria set out in the Better Regulation guidelines**[156], analysing to which extent the existing policy and legislative framework is effective (in terms of results and impacts), efficient (in terms of implementation costs), relevant to the needs, coherent with other EU and international measures and has demonstrated an EU added value. Specific **evaluation questions** are answered.

[155] Along the study victims' rights refer mainly to individuals that are victims of fraud
[156] SWD(2015) 111 final

www.parlament.gv.at

- Time: the report covers the implementation of the Framework Decision since 2001 (date of the adoption) to 2016.

- Stakeholders:
  - Law Enforcement Agencies (LEAs);
  - National Banking Federations;
  - Private sector including: Banking system, Cards schemes, Card mobile payment services, Peer-to-peer mobile payment services, Internet payment companies, Third party providers, Money transfer companies, Airlines companies, E-commerce companies, Commercial platforms (e.g. eBay, Amazon), Retailer's associations
  - Judiciary;
  - Data Protection Authorities (data protection authorities) and other stakeholders active in the area of data protection including: stakeholders in the field of data protection, Stakeholders in the field of fundamental rights, Victims' and consumers' associations, Academia;
  - legal practitionerss – defence lawyers;
  - public-private partnership representatives;
  - EU Institutions and bodies

- Territory: EU28 Member States (thus including the UK that has opted out from transposing the Framework Decision and SI that has not notified COM on transposition),[157] with a specific focus on 10 Member States (DE, FI, FR, IE, IT, NL, PL, PT, RO, UK).

3. Background

This section outlines the situation at the time the Framework Decision was adopted and presents an overview of the Framework Decision 2001/413/JHA and its intervention logic and of the broader EU and international policy.

Baseline

In 2001,[158] at the time in which the Framework Decision has been adopted, the level of cross-border fraud was already higher than that of domestic fraud[159] and migration of fraud towards the digital environment was already a concern.

[157] See https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=68

[158] Data referred to in this section is included in the Commission Communication "Preventing fraud and counterfeiting of non-cash means of payment", COM(2001) 11 final of 9.2.2001

[159] In the top ten issuing countries of the EU-15 the rate of cross-border fraud for payment cards was several times higher than the overall EU fraud rate and in some third countries, the cross-border fraud rate was even higher.

Proceeds of criminal activities linked with non-cash payment fraud was estimated at €600 million in the EU-15 (roughly corresponds to 0.07% of the payment cards turnover in the European Union), growing by approximately 50% last year.

Although sophisticated techniques were already used to commit payment fraud on the Internet, these have been evolving throughout the years.

The Framework Decision 2001/413/JHA

The Council Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment provides common minimum rules for the definition of fraud and counterfeiting of non-cash means of payment and for the related sanctions/penalties. The Framework Decision aims at ensuring a high level of protection through criminal-law against fraud committed through and counterfeiting of non-cash means of payment against in all Member States and requires them to take measures to achieve the intended outcome.

The Framework Decision is part of the first EU Fraud Prevention Action Plan 2001,[160] aiming to improve the prevention of fraud and counterfeiting of all non-cash payments among the Member States, especially by extending the cooperation and exchange of information for investigation and prosecution between the competent authorities of the Member States and by boosting the fraud prevention measures also in the third countries.

Rationale of the key provisions of the Framework Decision

Definition of payment instrument (Article 1)
Any physical ("corporeal") payment instrument which can be used to transfer money or monetary value and is protected against imitation or fraudulent use. The Framework Decision includes a non-exhaustive list of payment instruments (i.e. cards, cheques, travellers' cheques, bills of exchange). Even if it does not explicitly mention forms of value transfer such as wire transfers, direct debit, ticket restaurant, fidelity/loyalty cards, or coupons, these fall into its scope only when they are corporeal, used to transfer money or monetary value and protected against imitation or fraudulent use at least through a unique issuing number or their design. These forms of value transfer are then partially covered by the Framework Decision.
Criminal offences (Articles 2-4)
The Framework Decision identifies different forms of behaviours requiring criminalisation in relation to fraud and counterfeiting of non-cash means of payments with the aim that such behaviours are classified as criminal offences in all Member States and sanctioned

[160] Commission Communication "Preventing fraud and counterfeiting of non-cash means of payment", COM(2001) 11 final of 9.2.2001.

accordingly:

- **Offences related to payment instruments**[161]. Namely: (a) theft or other unlawful appropriation; (b) counterfeiting or falsification for fraudulent use; (c) receiving, obtaining, transporting, sale or transfer to another person or possession of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument in order for it to be used fraudulently; (d) fraudulent use of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument (*Art. 2*).
- **Offences related to computers** which consist in performing or causing a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by: (a) without right introducing, altering, deleting or suppressing computer data, in particular identification data or (b) without right interfering with the functioning of a computer programme or system (*Art. 3*).
- **Offences related to specifically adapted devices** which refer to the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of: instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsification of a payment instrument in order for it to be used fraudulently; computer programmes the purpose of which is the commission of any of the offences related to computers (*Art. 4*).
- **Participation, instigation and attempt** (*Art. 5*).

Legal person liability (Article 7)

The Framework Decision extends liability to legal persons when criminal offences are committed by natural persons with specific powers of representation and invites legal persons to set appropriate control measures.

Penalties (Article 6) and Sanctions for legal persons (Art. 8)

The Framework Decision provides Member States with high-level guidelines to set penalties for covered offences. It leaves the Member States room to ensure that the forms of conduct listed by the Framework Decision are punishable, by stating that the criminal penalties should be "effective, proportionate and dissuasive", without imposing specific levels of sanction but clarifying that, at least in serious cases, penalties should involve the deprivation of liberty.

The Framework Decision requires that legal persons considered liable under Article 7 are punishable by criminal or non-criminal fines and may include other sanctions such as: (a) exclusion from entitlement to public benefits or aid; (b) temporary or permanent disqualification from the practice of commercial activities; (c) placing under judicial supervision; (d) a judicial winding-up order.

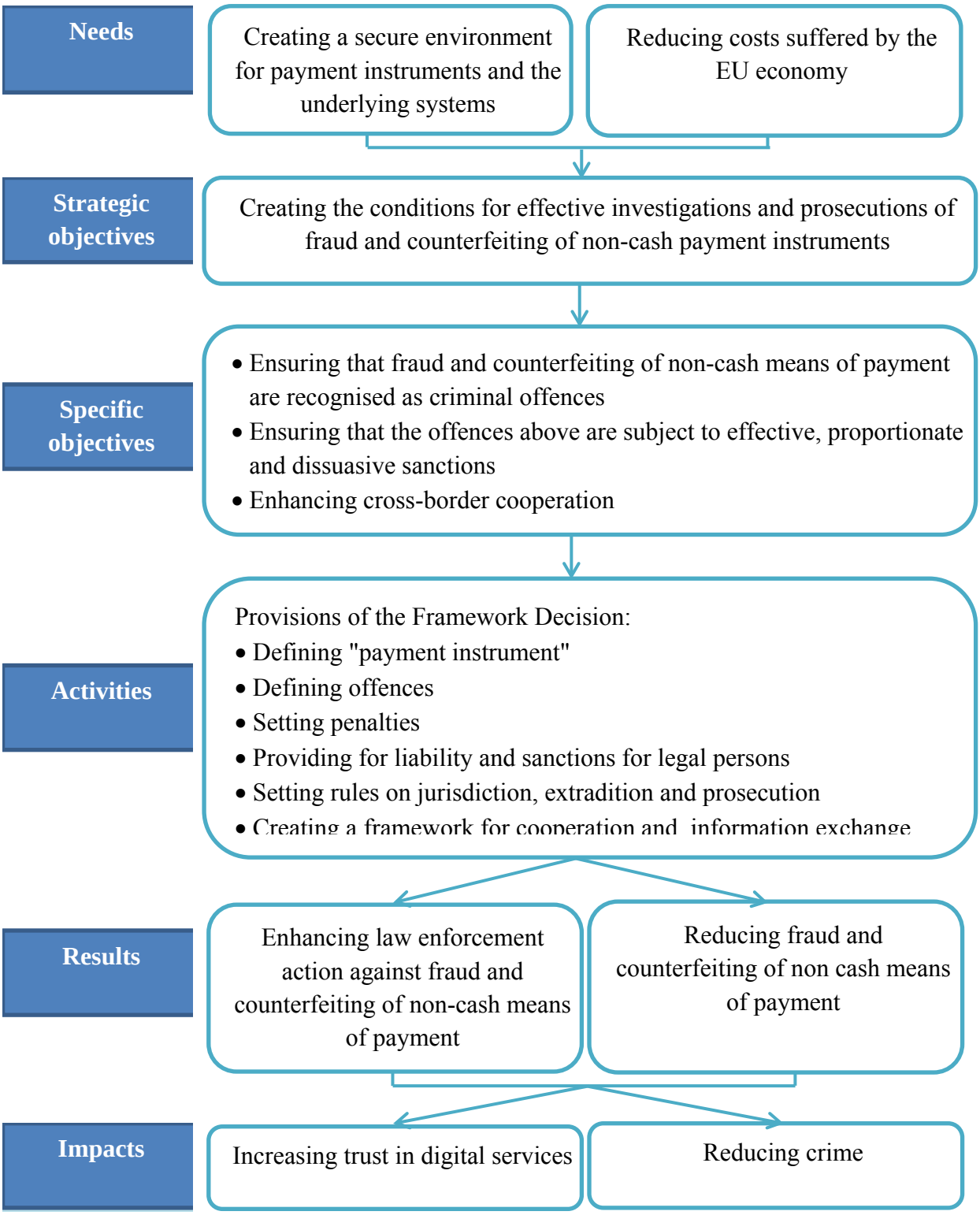
[161] In respect, at least, of credit cards, eurocheque cards, other cards issued by financial institutions, travellers cheques, eurocheques, other cheques and bills of exchange

Jurisdiction (Article 9)
The Framework Decision establishes that national jurisdiction on offences relating to non-cash payment applies if one of the following criteria is met: i) principle of *territoriality* (i.e. the country declares its competence on the offences committed in whole or in part within its territory); ii) principle of *personality* (i.e. the offences are committed by a Member States national) and principle of *dual criminality* (i.e. the national criminal law applies to the offences committed abroad, only if the criminal law of the Member State 1 applies to offenses committed outside the country by a national or a legal entity set up in that Member States, if the act is considered as an offense in the criminal law of the Member State 2/third country where it was committed or if it was committed in a place that is not subject to the jurisdiction of any state); iii) when the offences are committed for the benefit of a legal person that has its head office in the territory of that Member State. Member States may, however, decided not to apply criteria i) and ii) or limit them to specific cases.
Extradition and prosecution (Article 10)
The Framework Decision builds on the 1957 European Convention on Extradition which firstly introduced the right of Member States not to extradite their nationals. It disciplines cases in which a Member States decides not to extradite its nationals who have committed/are alleged to have committed outside its territory one of the criminal offences in scope of the Framework Decision. The rationale of this article is thus to create conditions for judicial cooperation between Member States in order to ensure that fraudsters are punished and Member States affected by the criminal offence are aware of the measures established and of the outcome of the prosecution.
Cross-border cooperation and exchange of information (Article 12)
In order to ease the implementation of the criminal law framework set through the previous provisions, the Framework Decision invites Member States to provide mutual assistance in criminal proceedings and to consult with each other in case more than one Member States has jurisdiction on the same case. The nomination of national contact points specifically dedicated to the exchange of information is also envisaged to facilitate cross-border investigations and prosecutions.

The intervention logic

The figure below illustrates a map of the intervention logic of the Framework Decision, displaying its provisions in relation to the strategic and specific objectives, as well as the causal links between the different levels.

Figure 1: intervention logic of the Framework Decision



The **strategic objective** of the Framework Decision is to create the conditions for effective investigation and prosecution of fraud in and counterfeiting of non-cash means of payment, in order to address two specific **needs**:

- Creating a secure environment for payment instruments and the underlying system[162]
- Reducing costs stemming from fraud and counterfeiting of non-cash means of payment suffered by the EU economy

The strategic objective has been operationalised into three **specific objectives:**

- Ensuring that fraud and counterfeiting of non-cash means of payment are recognised as criminal offences (Recital 4 of the Framework Decision)
- Ensuring that the offences above are subject to effective, proportionate and dissuasive sanctions (Recital 4 of the Framework Decision)
- Enhancing cross-border cooperation (Recital 11 of the Framework Decision)

In order to allow Member States to achieve these specific objectives, the Framework Decision includes key provisions to be implemented by Member States: specific forms of conduct to be criminalised, conditions for the liability of legal persons, setting rules regarding the level of penalties, defining principles for establishing jurisdiction, ruling cases of non-extradition, and defining rules for cross-border cooperation.

The correct and full implementation is directed at achieving specific **results**: a reduction of fraud and counterfeiting of non-cash means of payment; a stronger law enforcement action against crime (at national level as well as cross-border).

In the long term, the intended **impacts** of the provisions of the Framework Decision are: increasing public trust in digital services and reducing crime.

The achievement of these impacts is also affected by contextual factors such as: the reporting of the crimes to Law Enforcement Authorities (LEAs), public-private cooperation initiatives, and the level of protection granted to victims.

4. Evaluation Questions

EQ1. How much do fraud and counterfeiting of non-cash means of payment cost? To which entities? How are costs expected to increase?

EQ2. Can earnings for organised crime groups be quantified?

EQ3. What is the significance and evolution of identity theft in this context?

EQ4. Is the scope (definition of "payment instrument") of the Framework Decision still valid, taking into account technological developments? Are newer forms of "value transfer",

[162] Communication from the Commission to the European Parliament, the Council, the European Central Bank and the Economic and Social Committee - A framework for action on combatting fraud and counterfeiting of non- cash means of payment (COM/98/0395 final)

including non-corporeal means of payment, covered by national legislation? (E.g. mobile payments, centralised and decentralised virtual currencies, fidelity/ loyalty cards, fuel cards, commercial cards, coupons, prepaid debit cards)? Are newer forms of crime covered by the current provisions in the Member States, as, for instance (but not only): phishing, collecting data, trafficking of (stolen) credentials (for instance on carding websites), acting as money mule. (*Relevance*)

EQ5. What is the level of transposition and implementation of the Framework Decision in EU Member States? (*Effectiveness*)

EQ6. Is there a need to improve co-operation among law enforcement authorities/judicial authorities and, if so, how could this be achieved? (*Effectiveness, Coherence*)

EQ7. What are the obstacles to investigations and prosecutions? (*Effectiveness*)

EQ8. How is the issue of territoriality overcome? Is there a need to expand jurisdiction (e.g. extra-territorial jurisdiction)? (*Effectiveness*)

EQ9. To which extent the objectives of the Framework Decision have been met? Has crime become less frequent? Have investigations, prosecutions and convictions increased? Have organised crime groups been disrupted? Or obliged to "migrate"? (*Effectiveness*)

EQ10. To which extent the individuals are affected by the use of their fraudulently acquired payment (card) data? What are the actual and potential consequences for the individuals? (e.g. causing a financial loss and exposing the individual to negative credit ratings or other negative consequences of identity theft) (*Effectiveness*)

EQ11. What are the specific needs of victims of fraud and/or identity theft? (*Effectiveness*)

EQ12. How is the victim protected by existing rules? (*Effectiveness*)

EQ13. Is reporting to law enforcement of the crimes defined by the Framework Decision compulsory under Member States' national laws? (*Effectiveness, efficiency*)

EQ14. Do law enforcement authorities consider the level of reporting satisfactory? (*Effectiveness, efficiency*)

EQ15. Is public-private co-operation structured to effectively and efficiently meet the Council Decision's objectives? (*Effectiveness, efficiency*)

EQ16. Are there any overlapping/contradictions/complementarities between the Framework Decision and any other relevant EU/international legislation? In particular: the Revised Payment Services Directive, the Directive on Network and Information Security, the Directive on attacks against information systems, the Directive establishing minimum standards on the rights, support and protection of victims of crime, the Directive on the protection of the euro and other currencies against counterfeiting by criminal law, the Interchange Fee Regulation. (*Coherence*)

EQ17. What is the added value resulting from the EU intervention compared to what could be achieved by Member State action only? (*EU Added value*)

EQ18. To what extent does the Framework Decision support and usefully supplement Member State's policies in relation to fraud and counterfeiting of non-cash means of payment? (*EU Added value*)

5. Methodological approach

The evaluation relied on:

- the reconstruction of the Framework Decision intervention logic, showing the objectives of the intervention and the chain of expected effects (outputs, outcomes and impacts);
- desk research on EU and national information;
- field research, including interviews, a web based survey targeted to National Banking Federations, law enforcement agencies, associations and data protection authorities and the private sector, and a validation focus group.
- the results of the open public consultation that the European Commission launched in March 2017 to collect opinions on the effectiveness of the current legislative and policy framework and on existing problems and possible options for future initiatives.

Please see annex 2 for more information on the results of the consultation.

Limitations:

- It was not possible to quantify the extent to which the Framework Decision has contributed to reducing the level of fraud. The estimates of cross-border fraud at the time of the adoption of the Framework Decision were around EUR 600 million and in 2013 the total level of card fraud was EUR 1.44 billion (latest data available). However, it is not possible to meaningfully compare those figures, since the assumptions for the calculation of the situation in 2001 are unknown, apart from the fact that at that time almost half of the Member States it had in 2013 (15 vs 28).
  In addition, the total growth in fraud is likely to be the outcome of several concurring factors, from which it is impossible to quantitatively isolate the direct effect of the Framework Decision.
- The quantification of crime is hampered by i) the limited statistics available at EU level, ii) the fact that available statistics do not cover recent and emerging forms non-cash means of payment; iii) criminal statistics do not always identify crimes corresponding at the offences defined in the Framework Decision; and iv) unreported or undiscovered crime is an issue. In order to minimise the effects of these limits, the statistics were integrated with information gathered through other sources (such as industry reports and reports focused on specific countries) and with input provided by stakeholders consulted.

www.parlament.gv.at

- Lack of data on prosecutions and investigations and their impact on Organised Crime Groups limited the assessment of the effectiveness and added value of the Framework Decision and qualitative data had to be used.
- National judicial representatives proved to be particularly difficult to engage, and despite having expanded the original list and mobilised stakeholders and the network of national fraud experts this category remains poorly represented.
- The results of stakeholder consultations represent subjective views and opinions of those who chose to participate, often providing input on selected aspects of the study. As such, these data are presented as qualitative and not generalised to a wider population.

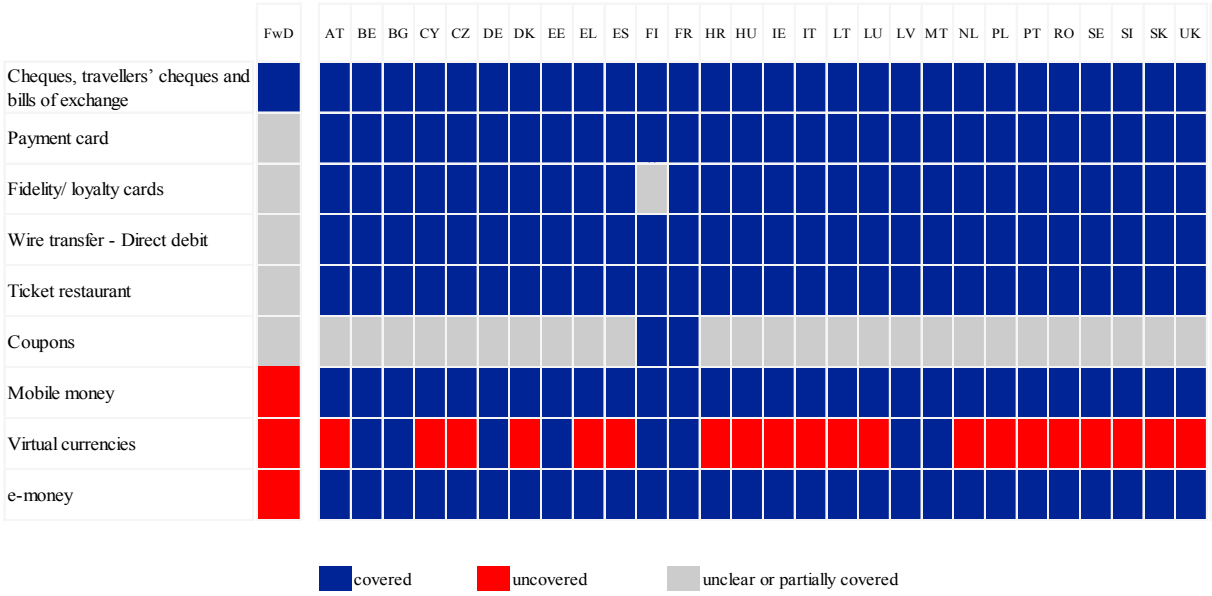
6. Implementation state of play (results)[163]

Investigation and prosecution: (criminal) law

- Definitions:

The definition of payment instrument in the Framework Decision has been implemented across all Member States. Furthermore, all Member States have adopted broader definitions than that of the Framework Decision, covering corporeal and non-corporeal payment instruments not explicitly mentioned in the Framework Decision (e.g. e-money, fidelity/loyalty cards, wire transfers, direct debits, and ticket restaurant).

Figure 2: implementation of Framework Decision definition of payment instruments



Source: EY

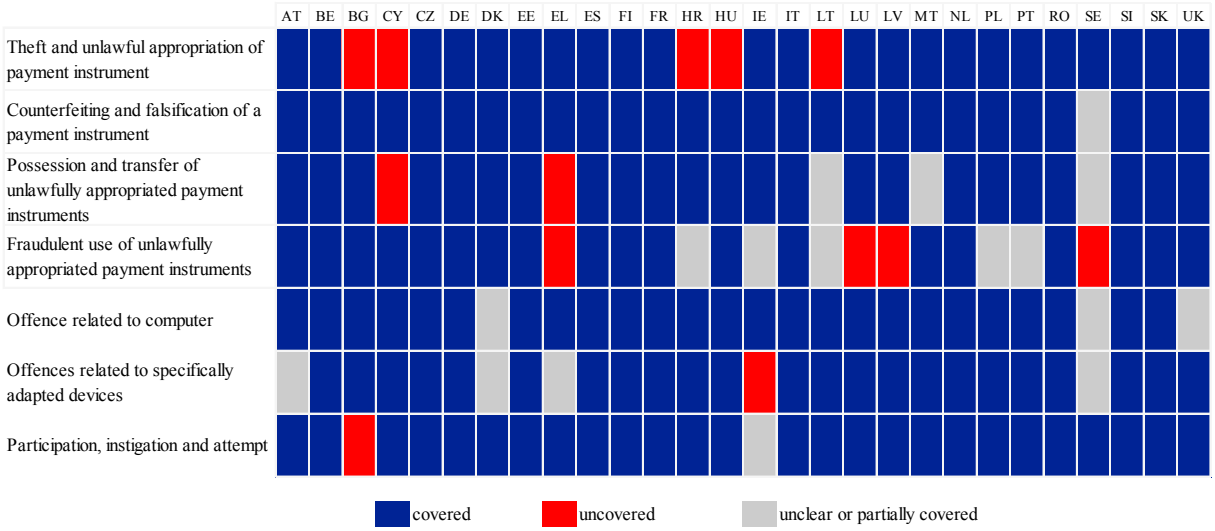
[163] The detailed transposition tables of the Framework Decision are annexed to the Study "Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combatting fraud in and counterfeiting of non-cash means of payment"

The definition of payment instrument in the Payment Services Directive has already been widely transposed, which explains why mobile money, and e-money are currently considered payment instruments by all Member States.

- Offences:

Member States have in general implemented the Articles in the Framework Decision describing the offences, with few exceptions:

Figure 3: implementation of Framework Decision offences



Source: EY

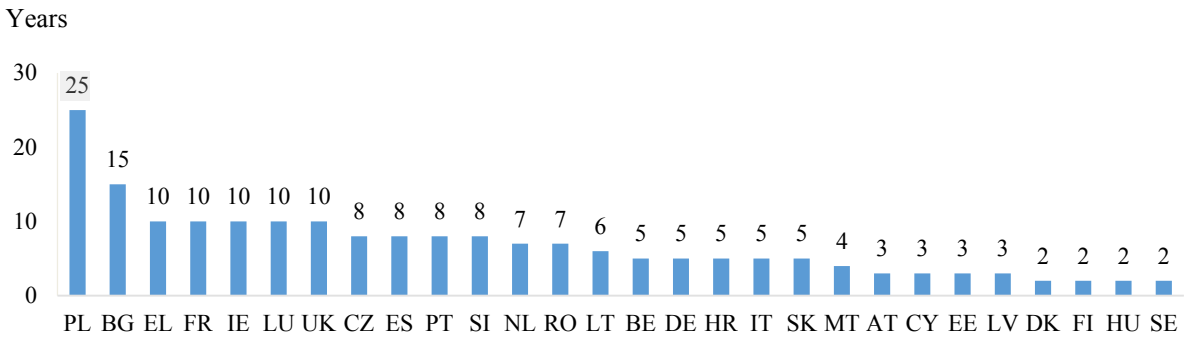
The offence with fewer Member States covering it fully is the fraudulent use of payment instruments (Article 2(d)) with 9 Member States not covering it or covering it only partially (e.g. the fraudulent actions do not refer specifically to payment instruments, but to currency or money, legal tender or documents, cheques, currency note or coin).

- Penalties:

Member States have adopted very varied levels of penalties for the offences contemplated in the Framework Decision.

Whereas all Member States include, at least for serious cases, penalties of imprisonment, these vary significantly. For example, figure 4 shows the variation in the level of maximum number of years of imprisonment for counterfeiting or falsification of payment instruments (Article 2(b)):

Figure 4: maximum penalties across Member States for Article 2(b) offences



Source: EY

This offence has the highest level of penalties in general. On the other side of the spectrum, the offences related to specific adapted devices (Article 4) are punished with the lowest levels of penalties.

- Legal person liability and sanctions:

Most Member States (21)[164] have fully transposed the Framework Decision provision relating to the liability of legal persons. FR, ES and RO have adopted broader definitions of "legal person", and wider criteria to trigger liability. Whereas the definition of legal person in the Framework Decision excludes "States or other public bodies in the exercise of State authority and for public international organisations" (Article1-(b)), FR and RO considers public authorities to be legal persons and therefore liable for offences committed by natural persons for the benefit of the legal entity. The Spanish legislation goes beyond the scope of the Framework Decision, restricted to specific positions inside the legal entity, and extends liability for legal person to all cases where the offence is committed in the course of its business and on its behalf and for its benefit, regardless of who commits the offences.

Five Member States transposed only part of this provision, not fully covering the criminal liability (DE, IT, and NL), the categories of persons who can trigger the liability (CY), or the conditions for liability of legal persons (PT). BG and LV do not recognise the liability of legal persons in cases of criminal offences relating to non-cash payment fraud.

All Member States except ES, BG, LV, and PT have transposed the sanctions for legal persons as provided by Article 8 of the Framework Decision (i.e. fines). ES and PT impose administrative measures.

[164] All except BG, CY, DE, IT, LV, NL, PT

Although the lack of harmonisation of sanctions for legal persons may be in theory an obstacle to prosecutions (e.g. in crimes committed for the benefit of a legal person based in a Member State that does not recognise the liability of the legal person and where the victim is based in another Member State), no evidence was found during the evaluation or in the consultation.

Investigation and prosecution: police and judicial cooperation

- Jurisdiction:

All Member States have implemented at least one of the principles for establishing jurisdiction set in the Framework Decision:

- All Member States adopted the territoriality principle (Article 9(a)). Many of them[165] expanded the interpretation of the principle by including situations such as when the consequences of the offence became apparent in national territory (FI) or when the offence is committed on a national ship or aircraft (DK).
- A majority of Member States[166] adopted the nationality and double criminality principles (Article 9(b)). Many of them[167] included additional situations, such as covering acts committed abroad by a person with no nationality, who has been granted a permanent residence in its territory (CZ), or the application of jurisdiction when the offender is a citizen of the country at the time of the perpetration of the offence (EE).
- A few[168] Member States chose to establish their jurisdiction when the offences are committed for the benefit of a legal person that has its head office in the Member State (Article 9(c)). Again, some of them widened their interpretation of the definition provided in the Framework Decision by extending national jurisdiction to offences committed for the benefit of legal persons that carry on business activities on their territory, without having established their head office there (e.g. CZ).

Besides the criteria set out in the Framework Decision, a few Member States have adopted additional criteria to establish their jurisdiction on non-cash payment fraud. These include the nationality of the victims (EE, SI) and the existence of damages/losses for the Member State caused by the criminal offence (SI).

Overall, a majority of Member States (22)[169] have extended their jurisdiction beyond the requirements of the Framework Decision in a variety of ways.

[165] CZ, DE, DK, EE, EL, FI, HR, LT, LV, MT, PL, PT, RO, SI, SK, UK
[166] AT, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, LT, MT, NL, PL, PT, SE, SI, SK, UK
[167] AT, CY, CZ, DE, DK, EE, ES, FI, FR, HU, LT, MT, SE, SK, UK
[168] CY, CZ, EE, ES, FI, FR, LV, MT, PT, RO, SE
[169] AT, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, LT, LV, MT, PL, PT, RO, SE, SI, SK, UK

www.parlament.gv.at

As pointed out in the expert meetings, these differences in the implementation increase the complexity of the attribution of jurisdiction of cross-border offences, may result in longer prosecution times and, in some cases, no prosecution at all (e.g. if no country claims jurisdiction).

- Extradition:

The European Arrest Warrant[170] as lex posterior partially makes the provisions above redundant, by setting conditions for compulsory extradition for offences covered by the Framework Decision (e.g. specifically "fraud, including that affecting the financial interests of the European Communities", "forgery of means of payment", "computer-related crime", "participation in a criminal organisation") when they are punished by a certain level of penalties. Member States can no longer refuse to extradite to another Member State citizens on the sole grounds of nationality, in case the offences committed are punishable by a custodial sentence or a detention order for a maximum period of at least three years. The European Arrest Warrant may apply for offences punishable by imprisonment or a detention order for a maximum period of at least 1 year or where a final custodial sentence has been passed or a detention order has been made, for sentences of at least 4 months. In these cases, the provisions of the Framework Decision coexist with the option left to Member States to issue and European Arrest Warrant.

Taking this into account, the scope of the implementation of the extradition provisions in the Framework Decision is limited to:

1) Member States (16)[171] that in general do not extradite their nationals.
2) Criminal offences with specific levels of penalties when there is not an obligation to extradite derived from the European Arrest Warrant.

In these cases, most Member States have put in place measures to establish their jurisdiction to ensure that no crime remains unpunished:

Table 1: overview of implementation of extradition provisions in the Framework Decision

[170] 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision

[171] AT, BE, CY, CZ, DE, EL, ES, FR, HR, LT, LU, LV, PL, PT, SI, SK, of which DE, EL, CZ, LT do not extradite its own nationals outside the EU

	Offences committed by its own nationals abroad (Art 10, Par. 1 let. a)	Offences committed by its own nationals abroad and refusal of extradition solely on nationality grounds (Art 10, Par. 1 let. b)
Member States with measures in place	AT, BE, CZ, CY, DE, EL, ES, HR, LT, LV, PT, SK, SI	AT, CZ, DE, HR, LT, LV, PT, SI, SK, BE, LU, ES, CY, PL
Member States without measures in place	FR, LU, PL	FR, EL

- Cross-border cooperation:

With regard to Article 11 of the Framework Decision, all Member States have adopted measures of mutual assistance in respect of proceedings related to the offences in the Framework Decision.

As for Article 12, Member States have designated dedicated operational contact points in charge of international cooperation that include officials in the Ministry of Justice, law enforcement representatives or their contact points in the European Judicial Network, Eurojust or Europol.

7. Answers to the evaluation questions

Relevance

The Framework Decision presents some shortcomings in terms of how relevant it is in terms of: 1) the definitions it is based on and 2) the way the offences are defined [EQ4].

Moreover, the Framework Decision falls short in addressing issues connected with non-cash payment fraud, such as identity theft [EQ3]

On the other hand, with regard to conditions for the liability of legal persons, the principles for establishing jurisdiction, and for ensuring prosecutions in case of non-extradition, the analysis and the stakeholder consultation confirmed the relevance of the Framework Decision.

1) Definitions

Recent years have brought not only an exponential increase in the digital economy but also a burst of innovation, including in payment technologies.

Innovative players (e.g. Google, Samsung, Apple…) have contributed to the development of disruptive solutions that aim to meet the growing expectations of consumers for immediacy and convenience, including in payment services.[172]

Innovative products like Mobile Points of Sale and the diffusion of technologies such as **contactless**[173] have contributed to increasing the use of cards in face-to-face transactions. With regard to technologies applied to mobile devices, the most relevant example relate to the spread of **mobile wallets**, which combine Near Field Communication technology with mobile devices (i.e. smartphones and tablets) used to virtualise and store payment cards or account information to be used as point of sales to make purchases.

The use of virtual currencies (e.g. Bitcoin) has also emerged in recent years. Compared to other payment instruments (in particular those used for international transfers, such as money remittances), virtual currencies offer:[174]

- Speed: a transaction confirmation takes approximately 10 minutes.
- Low cost: transactions can be processed for free.
- Micro payments: virtual currencies can be fragmented to very low amounts.
- Financial inclusion: international transfers with virtual currency wallets are cheaper (average cost of sending small remittances with traditional methods is 7%, vs 1% with bitcoin). [175]
- Security, trust and transparency through the use of distributed ledgers.

These new payment instruments contribute to an increase in fraud. For example, virtual currencies users can fall victim of fraud when a fraudulent wallet software pretends to be a solution for storing virtual currencies, while being designed to steal funds that the users manages with the wallet.[176] Virtual currencies users can also fall victim of phishing or other scams that are generally used in non-cash payment fraud.[177]

The definition of "payment instrument" contained in the Framework Decision does not appear to be fully relevant against the background of technological developments. Most of the stakeholders[178] consulted consider this definition to be only partially appropriate. EU Member States went beyond the provision of the Framework Decision, adopting wider and more

[172] The globalisation of immediate payments – rolling out faster transactions, Banking Tech, 2017
[173] At the end of 2015 there were 41% more contactless cards (i.e. 346 million) than in 2014 (Retail Banking Research, 2016)
[174] Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/ EC
[175] Virtual Currencies and Beyond: Initial Considerations, IMF Staff Discussion Note, 2016
[176] Other example of crime against virtual currency operators is the theft of more than $450 million from Mt. Gox, a bitcoin exchange, in 2014
[177] More information on the various types of fraud can be found here and an overview of the relevant bitcoin scams can be found here
[178] Feedback received through the targeted consultation

inclusive definitions, covering more types of non-cash payment instruments than the ones listed and covered by the Framework Decision.

The definition of "payment instrument" used in the Framework Decision appears to be outdated both in terms of what it covers (some of the means of payment included in the list of examples under Article 1, such as eurocheques and eurocheque cards, are obsolete) and what it leaves out: the use of non-corporeal forms of value transfer is growing fast and they are increasingly affected by fraudulent transactions. In this regard, stakeholders highlighted the growing importance of payment instruments such as: e-money, mobile money, virtual currencies (such as Bitcoin).[179]

> ⇨ Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised.

Moreover, other terms included in the Framework Decision lack of a specific definition, which impinges on the clarity of the scope of certain provisions: for instance, the Framework Decision does not define "computer system" (Article 3) or "computer programme" (Articles 3 and 4), which may for instance impinge on the capacity of law enforcement to act on crimes committed "in the cloud".

2) Offences

Non-cash payment fraud can take the following forms:

1) Trigger payments by using payer information in a fraudulent way. This stage includes 2 sets of behaviours: the collection (e.g. phishing, skimming), trade (e.g. carding websites), making available (e.g. dumping) and possession of payer information (**preparatory acts**) and the actual **use** of the payer information.

- The Framework Decision covers the **use** of the payer information to trigger the execution of the payment is covered by Article 3 ("… without right introducing, altering, deleting or suppressing computer data, in particular identification data…"). However, the use of unlawfully appropriated computer data covered by Article 3, is criminalised only when offences intentionally result in a **transfer of monetary value**. This means that all the **preparatory acts** that precede fraud without being directly linked to it are excluded from Article 3.

  Moreover, Article 4 covers the "fraudulent making, receiving, obtaining, sale or transfer to another person or the possession of **computer programmes** the purpose of which is the commission of any of the offences described under Article 3". Here appears again the issue of a lack of definition of a computer programme. Also, the use of these computer

[179] Feedback received through the targeted consultation

programmes is not explicitly mentioned and in some cases it may not be necessary to possess them to be able to use them (e.g. they might be used from the cloud).

Article 5 covers "attempting the conduct" but this does not cover the mere possession, distribution or procurement of payer information unless performing or causing a transfer of money or monetary value using the payer information has been attempted as well.

Experts from the Member States confirmed the need for a criminalisation at EU level of preparatory acts (in particular phishing), during the second expert meeting.

- The Directive on Attacks Against Information Systems[180] criminalises the "intentional production, sale, procurement for use, import, distribution or otherwise making available… of… a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.",[181] with the intention to gain illegal access to information systems by infringing a security measure.[182] As discussed earlier, a fraudster using legitimate (but stolen) credit card credentials to shop online would not necessarily infringe any security measures.

> ⇨ **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised.

2) Fraudulently execute payments by tampering with or stealing the payment instrument.

- The Framework Decision focuses on the criminalisation of tampering with or stealing the payment instrument.

    - Tampering:
        - Counterfeiting: Article 2(b)
            - Trading or possessing counterfeit instruments: Article 2(c).
            - Trading or possessing means to counterfeit: Article 4(first part)
        - Hacking of information systems to process payments: Article 3 (computers)
            - Trading or possessing means to hack: Article 4(second part)
    - Stealing: Article 2(a)
        - Use of stolen instruments: Article 2(d)

  The previous analysis and problems previously identified due to a lack of technology neutral definitions apply here as well (non-criminalisation of offences involving certain payment instruments not covered by the current definition).

[180] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
[181] Article 7(b)
[182] Article 3

3) Fail to provide the product/service after receiving the payment.

- The Framework Decision does not cover this type of conduct, which falls under the general definition of "fraud".

3) Identity theft [EQ3; EQ10]

Information related to the identity of a person is often used by criminals to commit fraud or any crime of financial nature. In the 2004 Action Plan on payment fraud prevention,[183] identity theft was already highlighted as a growing issue together with the need to strengthen business and consumer confidence in the use of non-cash means of payment.

It is hard to quantify volumes and values of identity related crimes, because:

- There is no common definition for identity theft
- The notion of "victims" is unclear, covering individuals, governments, international organisations, business and/or industry, or the economy as a whole and do not measure the same types of fraud or crimes and are thus not comparable.[184]
- Companies and businesses are reluctant to share data, given the perceived risks of undermining their reputation (hence losing potential business opportunities) and drawing attention on the vulnerabilities of their systems.[185]

Victims of identity theft can suffer financial losses, reputational damage, psychological and social distress, impacts on fundamental rights (e.g. data protection and privacy) and costs to rectify the consequences of the theft (e.g. replacing identity documents). Available data do not allow for the isolation of cases of identity theft generating economic losses or cases relating to non-cash payment fraud.

When focusing on **individuals as primary victims**, in 2012 identity theft[186] affected around 8.2 million people across Europe, equal to 2% of the EU population.[187] A recent Special Eurobarometer on Cybercrime further highlighted the relevance of the problem. Most EU Internet users (68%) are concerned about being victims of identity theft and concern is growing quickly (+16% from 2013 to 2014). On average, 7% of European Internet users claimed to have been victims of identity theft.[188]

[183] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee, the European Central Bank and Europol of 20 October 2004 - A new EU Action Plan 2004-2007 to prevent fraud on non-cash means of payment [COM(2004) 679 final
[184] OECD. (2008). Scoping paper on online identity theft. Retrieved from DSTI/CP(2007)3/FINAL
[185] Companies choosing not to report the number of records lost increased by 85% in 2015 (Symantec, 2016).
[186] According to the Center for Strategy & Evaluation Services it should include the cases "when any person acquires, transfers, possesses or uses personal information of a natural or legal person with the intent to make a false representation as to his identity to make a gain, acquire a benefit for himself or another, cause direct or indirect loss to another, expose another to a risk of loss, damage the reputation of another, expose another to a risk of damage to the reputation or mislead investigation relating to any crime" (European Commission, 2012).
[187] European Commission, Study for an impact assessment on a proposal for a new legal framework on identity theft (2012)
[188] Special Eurobarometer 423, Cyber Security, February 2015

Most of the Member States (at least 22)[189] acknowledge the relevance of the criminal phenomenon and cover identity theft by their national legislation, in some cases adding some legal pre-conditions.[190] Some national legislation identified the illegal origin of credentials as a condition for criminal action and underlined the need to cover all types of credentials. However, in the current situation only some national legislations have a definition of "credentials" while the majority requires proving their fraudulent use.[191]

Effectiveness

The specific objectives pursued by the Framework Decision are:

1. Ensuring that fraud and counterfeiting of non-cash means of payment are recognised as criminal offences
2. Ensuring that the offences above are subject to effective, proportionate and dissuasive sanctions
3. Enhancing cross-border cooperation

In general, data available does not allow for establishing any direct correlation between the entry into force of the Framework Decision and the dimension of crime [EQ9]. However, there is evidence that non-cash payment fraud has increased globally, both in absolute and in relative terms, over the last years. Investigations, prosecutions and convictions are in constant growth since 1990.

It is difficult to establish the level to which the Framework Decision contributed to the formation of current national legislative and procedural criminal law frameworks [EQ9]. Many of the provisions of the Framework Decision[192] are now complemented by provisions of other EU and international legislation which, in many cases, led Member States to modify their legislation and contributed to achieve the objectives of the Framework Decision.

As specified above (under "Relevance"), the Framework Decision appears to have lost its relevance in terms of ensuring that fraud and counterfeiting of non-cash means of payment are recognised as criminal offences (specific objective 1), due mainly to technological developments.

Moreover, as outlined in Section 6 of this report, some issues remain to be addressed to achieve a complete transposition of the Framework Decision. Some Member States have not

[189] AT, BG, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, IT, LT, LV, MT, NL, PL, PT, SE, SK, UK.
[190] For instance, some Member States (at least CZ, EE, FR, IT, LV, PT, SE) consider identity theft a crime only when it resulted in a damage (financial or other kind of social or psychological consequences) for the victim. As underlined in the 1st EGM, in EE identity theft is punishable independently from fraud-related provisions provided the condition of the damage is met. In MT, it is necessary to prove that the offender has fabricated non existing events and lies, PL considers identity theft a crime only upon the harmed party's motion while EL prosecutes identity theft *ex officio*.
[191] Inputs provided during the 1st Expert Group meeting.
[192] Art. 1 let.a; Art. 3; Art. 4; Art. 5; Art. 6; Art. 8 para. 1; Art. 9 para. 1 let. A; Art. 9 para. 1 let. B; Art. 10 para. 1 let. A; Art. 11 para. 2.

www.parlament.gv.at

yet transposed fully some of the provisions (such as criminal offences, penalties, and liability of legal persons). The following **main problems linked with the implementation of the Framework Decision** [EQ5] have been identified:

1) disparate levels of criminalisation of offences (penalties - specific objective 2)
2) lack of timely exchange of information among law enforcement authorities (cross-border cooperation - specific objective 3)

1) Penalties:

The Framework Decision requires Member States to set up criminal penalties that are effective, proportionate and dissuasive, without specifying minimum levels. As a consequence, Member States have adopted different levels of penalties (see section 6).

Offences defined by Articles 2 to 5 of the Framework Decision are punished through specific penalties in most of the Member States. However, the Framework Decision failed to approximate the level of penalties for those offences across EU Member States.

- Organised crime groups are often responsible for non-cash payment fraud (see Section 1.2.3. of the impact assessment report, [EQ2]), moving their activities across the borders and operating in several Member States. Therefore, there is a risk of forum shopping (criminals moving to countries with a more lenient criminal law system).
- The disparate level of sanctions may have a negative impact on judicial cooperation. If a Member State has low minimum sanctions in its criminal code, this could lead to low priority given by law enforcement and judicial authorities to investigate and prosecute non-cash payment fraud. This can also have a negative impact for the cross border cooperation when another Member State asks for assistance, in terms of timely processing of the request. Disparities in sanction levels can be expected to benefit particularly strongly the most serious offenders, i.e. transnational organised crime groups which have operative bases in several Member States.
- A European Arrest Warrant (EAW) may be issued by a national judicial authority if the person, whose return is sought, is accused of an offence for which the maximum period of the penalty, according to the law of the issuing Member State, is at least one year in prison or if he or she has been sentenced to a prison term of at least four months. The disparities within the punishments makes it difficult to request an EAW, due to the lack of a coherent level of sanctions, especially as regards to offences relating to receiving, obtaining, transporting, sale, transfer or possession of payment instruments. On the other hand, it can be deducted from the requirements for the content of the European Arrest Warrant that harmonised sanction levels facilitate execution of a warrant because they would avoid to a certain extent diverging interpretations of proportionality issues in the Member States concerned. [EQ16]
- In some EU Member States, forms of non-cash payment fraud are still not dealt with by means of investigative tools that are typically used for organised crime and transnational cases. This circumstance has a strong impact in the weakness of investigation and prosecution and leads to insufficient international cooperation between the Member States. Moreover, once investigations on non-cash payment fraud cases are started abroad with

particular investigative techniques, it is not possible to continue them in the same way when they arrive in a Member State whose legislation lacks provisions on these techniques.

- Finally, the recognition or the execution of a European Investigation Order (EIO) could be dependent on sanctions available since Article 11.1(g) provides for grounds for refusal of the recognition or execution of an EIO by the executing State if "the conduct for which the EIO has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex D, as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years". [EQ16]

Penalties established for criminal offences defined by the Framework Decision are perceived to be somewhat effective by stakeholders.[193] Private sector representatives were the most dissatisfied category of stakeholders, especially because of poor enforcement. Most of the stakeholders agreed that it is necessary to have more coherent level of penalties for offences related to non-cash means of payment across the EU.

- The Attacks against Information Systems Directive determines maximum level of penalties of at least 2 years for the offences it contemplates (illegal access to information systems, illegal system interference, illegal data interference, illegal interception, offences related to tools for committing offences and inciting, aiding, abetting and attempt). It also determines maximum level of penalties for aggravating circumstances from at least 3 years to at least 5 years, depending on the situation. [EQ16]

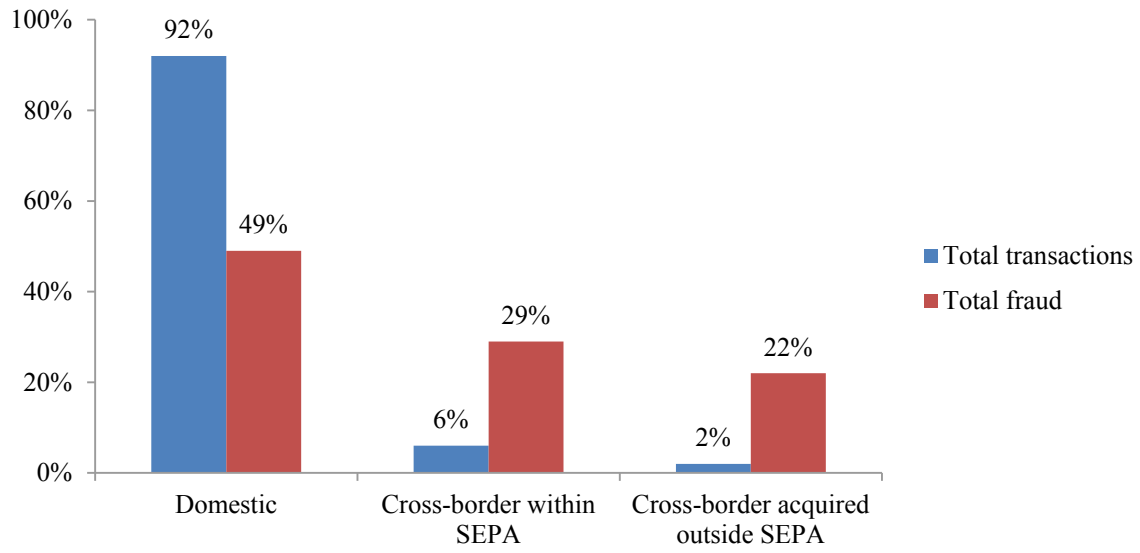
> ⇨ Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States.

2) Cross-border cooperation [EQ6, EQ7]

Card fraud has a disproportionate **cross-border** nature: whereas only a fraction of the transactions (<10% in value) are cross-border (within and outside SEPA), they account for half of the total fraud. The disproportion is particularly significant for transactions acquired from outside SEPA (2% in value), which account for 22% of all fraud:

Figure 5: value of domestic and cross-border transactions and fraud (2013)[194]

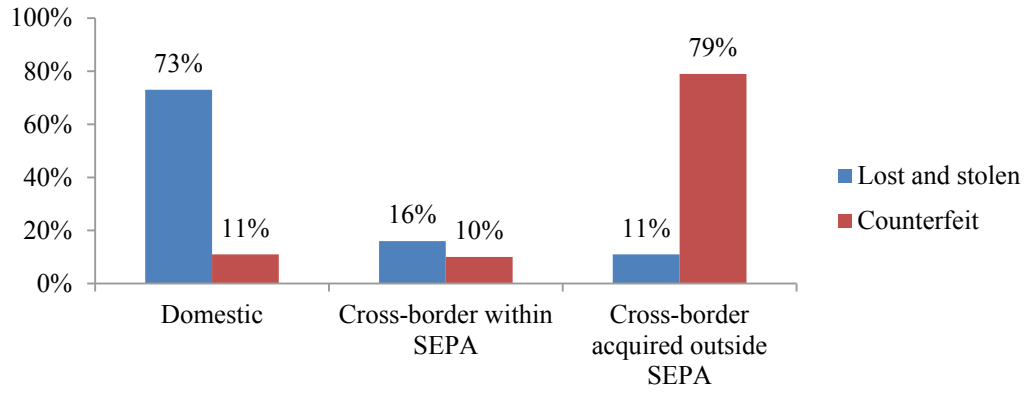
[193] Feed-back from targeted consultation
[194] This geographical composition varied little in the years prior to 2013 and is likely to remain similar today



Source: European Central Bank, Fourth Report on Card Fraud, 2015

In the case of card-present fraud (i.e. ATMs and POS terminals), one of the factors that explain the disproportionately high share of cross-border fraud committed outside SEPA is the preference among fraudsters to exploit low security standards, such as magnetic stripe technology in the case of counterfeit fraud:

Figure 6: geographical composition of card-present fraud (ATMs and POS terminals, 2013)[195]



Source: European Central Bank, Fourth Report on Card Fraud, 2015

The cross-border nature increases the pool of potential victims, makes it more difficult for victims to access their rights, facilitates the transnational operation of organized crime groups and complicates investigation and prosecution.

Box 1: the cross-border nature of non-cash payment fraud

[195] This geographical composition varied little from 2012 and is likely to remain similar today

In 2013, criminals from 27 countries around the world worked together to steal more than $45 Million in cash from ATMs, using counterfeit cards.

Criminals from Eastern Europe broke into the network of credit card processors in India and the United Arab Emirates, stealing prepaid card numbers and removing their withdrawal limits. They then used criminal networks to have counterfeited cards made with the stolen credentials and distributed the cards to hundreds of criminal groups around the world, who agreed on a date and time to hit simultaneously as many ATMs as possible. During the 10 hours that the joint robbery last, criminals carried out 36,000 ATM operations in 27 countries, walking away with over $45 Million in cash.[196]

There are a number of instruments for cross-border cooperation relevant to non-cash payment fraud already available in the EU:

Box 2: cross-border initiatives relevant to non-cash payment fraud

- FIU.NET Platform, supported by Europol and the European Commission. This platform supports the exchange of information between the 28 Financial Intelligence Units of the EU Member States in the fight against money laundering and terrorism financing.
- European Multidisciplinary Platform Against Criminal Threats (EMPACT)[197], "Cybercrime Card Fraud" priority, led by Europol and supported by the European Commission, CEPOL, Eurojust, Interpol and Norway, facilitates the cooperation of national law enforcement agencies in the implementation of joint operational actions, such as the Global Airline Action Days previously described.
- The European Judicial Cybercrime Network: The Network aims at facilitating and enhancing cooperation between the competent judicial authorities dealing with cybercrime, cyber- enabled crime and investigations in cyberspace, by facilitating exchange of information and best practice, as well as fostering dialogue among the different actors and stakeholders that have a role in ensuring the rule of law in cyberspace. This network was set up by the conclusions of the Council of the European Union on the European Judicial Cybercrime Network of 9 June 2016 (10025/16):
- Joint Investigation Teams (JIT) are investigative teams set up for a fixed period and for a specific purpose, based on an agreement between or among two or more law enforcement authorities in EU Member States. Competent authorities from countries outside the EU may participate in a JIT with the agreement of all other participating parties.
- The Asset Recovery Offices (AROs) platform enables co-operation on the recovery of the proceeds of crime.
- EU Cybercrime Task Force (EUCTF) is an inter-agency group formed by the heads of the national cybercrime units, Europol, the European Commission, CEPOL, Eurojust, Interpol, Norway, Switzerland and Iceland. It discusses the strategic and operational issues relating to cybercrime investigations and prosecutions at EU level.
- Anti-Fraud Coordination Structures (AFCOS) facilitates cooperation and exchange of information (including operational information) between the Member States, and with

[196] See here for more information
[197] See here for more information

OLAF in the fight against fraud.

- The Camden Asset Recovery Inter-Agency Network (CARIN) is an interagency network of law enforcement and judicial practitioners from 53 jurisdictions and 9 international organisations, with its General Secretariat within Europol, specialised in the field of asset tracing, freezing, seizure and confiscation of the proceeds of crime.

Stakeholders pointed out during the evaluation and consultation to a number of **obstacles** to cross-border cooperation, which basically boil down to the fact that **it takes a long time to receive the information requested from another Member State,** when that information is received at all:

1) First, it takes time to **set up the procedure** to exchange the information between the Member States, in particular when this requires the authorisation of multiple authorities.

2) Second, it takes time for the Member State asking to **understand** what can be requested, and for the Member State asked what is being requested (including the urgency of the request), given the significant differences that still exist in their legislative frameworks, such as those concerning:
   a. **Prescription periods**, both in terms of duration and of the moment the period starts to count (e.g. when the offence is completed or when the victim discovers the fraud). The duration is usually linked to the severity of the maximum penalties, which, as discussed, vary significantly across Member States.
   b. **Data retention** rules, following the 2014 sentence of the Court of Justice of the European Union[198] declaring invalid the Data Retention Directive[199], as well as **data protection** rules (the current Directive 95/46/EC will be repealed and replaced by the General Data Protection Regulation[200] in May 2018; the current Framework Decision 2008/977 will be repealed by the Data Protection Directive for the police and criminal justice sector[201], to be transposed by Member States by May 2018).
   c. **Confiscation rules**: while some Member States follow a "follow-the-money" approach and prioritise the asset recovery, other focus on tracking and retaining the perpetrator

.

[198] See the press release here

[199] Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[200] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[201] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

3) Last but not least, it takes time to **produce** the information requested:
    a. The information may not be **ready available**. When the information needs to be collected in the Member State, there can be **coordination issues** at the national level between law enforcement and judicial authorities for the exchange of information.
    If an **investigation** needs to be open to collect the information, a new set of issues appears, such as:
        - Lack of adequate **investigative tools**, in particular to investigate fraud with a cybercrime component (e.g. IT forensics, decryption, attribution).
        - Lack of **skills** in law enforcement and the judiciary to deal with non-cash payment fraud cases of certain technological sophistication.
        - Limited **capacity** of law enforcement, which causes other criminal offences to be prioritized over non-cash payment fraud (compared to other criminal offences, non-cash payment fraud is underreported, frequently involves a high volume of small financial losses, and a relatively low level of penalties).

    Also, the lack of **public-private sector cooperation** can hinder the ability to collect information promptly.
    b. When the information involves **third countries** outside of the EU, as is often the case in e.g. skimming and counterfeiting of credit cards, a new level of complication and delays is added.

Stakeholders emphasized multiple times the important role that Europol plays in helping overcome each of these obstacles, setting up communication channels, helping understand the requests and supporting Member States with its analytical capabilities and technical expertise.

> ⇨ It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution.

* * * *

Other issues **hampering the effectiveness of the current legal framework are linked with the scope of the current policy/legal framework**:

1) Issues related to the attribution of jurisdiction [EQ8]
2) Victims do not always receive adequate assistance [EQ10, EQ11, EQ12]
3) Criminals exploit the lack of awareness of victims. [EQ10, EQ11, EQ12]
4) Under-reporting to law enforcement due to information sharing gaps in public-private cooperation hampers investigations and assistance to victims [EQ13, EQ14, EQ15]

1) Jurisdiction [EQ8]

The Framework Decision specified a limited set of situations in which a Member State could claim jurisdiction: when the offence was either committed in its territory or abroad by one of its nationals (on condition of double criminality, i.e. provided that it was also an offence

abroad) or for the benefit a legal person stablished in its territory. The last 2 situations could be optional based on whether the Member State extradited its nationals, a possibility that the European Arrest Warrant has rendered partially obsolete (see extradition section below).

The biggest challenge concerning jurisdiction in non-cash payments is the cross-border nature of the crime combined with the access to digital evidence, as more and more non-cash payments fraud has a digital component. In cybercrime cases that include elements of non-cash payment fraud, the conduct may thus include a foreign element because they are often committed using information systems outside the territory from where the offender is physically located in or vice versa, or have consequences in a third country where also the evidence may be located in. The Framework Decision does not specifically address the issue of claiming jurisdiction when crimes takes place in information systems outside the territory of the (Member State) location of the offender or in situations where the offender is located in the same territory but the crime is committed using information systems in another country. Member States may exercise jurisdiction if one aspect of territorial competence is fulfilled, e.g. where (part) of the offence is committed, including, where damage is part of the offence, where damage occurred. Positive or negative conflicts of jurisdiction cannot be excluded depending on whether several countries claim jurisdiction over the same offence or none is claiming it. Unfortunately the latter may be often the case. Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings provides for procedures and remedies to solve such conflicts of jurisdiction.

To give an idea of the complexity of the issue, please consider the case of Hans, a **German** national working and living in **Poland**, where he has his bank account. Unfortunately, while on vacation in **Romania**, his credit card details were stolen via skimming when he paid a taxi that was cooperating with an organized crime group. This group sold his credit card details to a carding website hosted in the **Netherlands**, where a **Portuguese** national bought his card details for just €20. He later used them from his apartment in **Italy** (or at least from an IP address that pointed to Italy but he might very well have used a VPN to connect from his summer house in the Portuguese Algarve), to buy goods online in a website hosted in **France** (but belonging to a multinational company based in **Ireland**) to be shipped from **Spain** to his cousin in **Luxembourg**.

While this is a fictional case, representatives from law enforcement, judiciary and the private sector described in the expert meetings similar situations, involving as many jurisdictions, to illustrate the challenges they face while investigating non-cash payment fraud. The main risk is that crimes might not be investigated because no country claims jurisdiction or that the lack of judicial cooperation makes the cross-border investigation process impossible in practice.

The Framework Decision provides limited tools to address these challenges. For example, coming back to Hans, when he sees the illegal activity in his credit card and informs the Polish authorities, they would not be able to claim jurisdiction on the basis of the Framework Decision only (offence neither committed in its territory nor by one of its nationals not for the benefit of a legal person established in Poland).

Europol is one of the coordination centres in the framework of the Global Actions against online fraudsters in the Airline Sector, targeting criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data.[202] Global Actions have started in 2014 and take place once or twice a year. During those actions, Europol encountered two cases that illustrate difficulties in prosecution of criminals, due to jurisdiction issues.

Box 3: jurisdiction issues linked with airline ticket fraud

Case 1 – The suspect (national of **EUMS-A**) was travelling with a ticket booked *legally*, but purchase with collected miles obtained via illegal past bookings; the suspect was stopped at the arrival in **EUMS-B** (from **EUMS-C**) and found in possession of 1000+ credit cards credentials ("dumps") in his/her laptop computer. The suspect was known for having purchased plane tickets using compromised credit card credentials in the past.
The credit cards had with no links to **EUMS-B** and -due to the lack of a) specific provisions and b) links **EUMS-B** - prosecution was not possible; the transfer of the prosecution to **EUMS-C** was not possible either.
Case 2 – The suspect travelling using a ticket booked fraudulently but with no links to the EUMS where he/she was stopped;

- Nationality of the Airlines: **EUMS-A**;
- Credentials misused: compromised credit cards credentials issued by a bank based in **EUMS-B**;
- IP address used during on-line booking: from **EUMS-C**;
- Nationality of the passenger: **EUMS-D**;
- Physical presence of the fraudster: when Airlines noticed the fraudulent transaction the suspect was flying from **EUMS-E** via **EUMS-F** to **EUMS-G**

Legislation in EUMS-G does not allow prosecution for crimes not committed in EUMS-G (which was clearly not the case). Transfer of the prosecution to the country of where the offence was committed remains possible (EUMS-C or Member States where the suspect purchased the flight ticket).

The Attacks Against Information Systems Directive includes broader jurisdiction rules than the Framework Decision, by, for example, eliminating the condition of double criminality and including situations in which the offender is physically present in the Member State, regardless of whether the information system attacked is in the same Member State, and vice versa, when the information system is in the Member State, regardless of where the offender is located.

The Commission committed in 2016 to addressing the challenges for investigations in cyber-enabled crimes in its Communication on Delivering on the European Agenda on Security[203], aiming to propose solutions by the summer of 2017 [EQ16].

[202] For the latest Action: https://www.europol.europa.eu/sites/default/files/documents/operation_airline_action_day_2017.pdf
[203] COM(2016) 230 final

In its Conclusions on improving criminal justice in cyberspace,[204] adopted on 9 June 2016, the Council supported the Commission´s commitment and called on the Commission to take concrete actions based on a common EU approach to improve cooperation with service providers, make mutual legal assistance more efficient and to propose solutions to the problems of determining and enforcing jurisdiction in cyberspace.

The Commission conducted an expert consultation process and summarized its results in a non-paper,[205] presented to the Council on June 8 2017, which may result in a legislative initiative.

> ⇨ Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution**.**

2) Assistance to victims

The Framework Decision does not contain any provision concerning assistance to victims.

The Victims Directive[206] focuses on the rights, support and protection of victims of crime **during criminal proceedings.** Also, it only covers natural persons. As discussed previously, legal persons are also victim of non-cash payment fraud.

The Payment Services Directive 2015/2366 (PSD2) improves the protection of consumers in case of non-cash payment fraud by harmonising the rules on liability on both payers (natural and legal persons) and payment institutions (legal persons). In case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of the transaction to the payer, unless suspicions based on objective grounds are raised regarding a fraudulent behaviour by the payment service user. It also includes the right of consumers to unconditional refund. [EQ16]

Representatives from victims' associations indicated in the consultation that the current measures on assistance to victims are not sufficient. Although there are not available statistics to show the extent to which victims have received assistance and accessed their rights, the limited satisfaction of stakeholders with the current situation was linked to the fact that **complaints reported to law enforcement were not investigated or not sanctioned in a timely way** (if at all), due to the challenges to investigation and prosecution described in this section. In addition, as discussed earlier, non-cash payment fraud is on the rise, and in new ways that are not covered by the current legislative framework. Also, victims may suffer the **consequences of identity theft**, which is not properly covered in the legislation, as outlined under the section "Relevance", above [EQ3].

[204] Council conclusions on improving criminal justice in cyberspace
[205] Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward
[206] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA

3) Awareness raising

The Framework Decision addresses prevention only in an indirect way. Recital 10 indicates that by criminalizing fraud related primarily to payment instruments with certain protection against imitation and abuse, the intention is to encourage operators to add that protection to more payment instruments, thereby encouraging prevention.

The Payment Services Directive (PSD2) contains a number of measures to enhance the security requirements for electronic payments and to provide a legal and supervisory framework for emerging actors in the payment market. [EQ16]

The Directive on Network and Information Security (NIS Directive)[207] increases the resilience of providers of critical infrastructures, who will be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure the security of their networks and information systems. [EQ16]

Stakeholders highlighted in the consultation the importance of prevention and the need to further develop it at the national and EU level. The current policy/legislative framework does not include specific provisions to encourage raising awareness, research and education programmes to reduce the risk of becoming a victim of fraud.

⇨ Criminals exploit the **lack of awareness** of victims.

4) Public private cooperation[208]

The Framework Decision does not include any provisions on public-private cooperation.

At the same time, stakeholders that contributed to the consultation widely considered public-private cooperation an enabler to tackle non-cash payment fraud across all levers: from reaction (investigation and prosecution and assistance to victims) to prevention, given that information concerning non-cash payment fraud is spread across multiple private sector actors.

Relevant to non-corporeal payment instruments, the EU Cybersecurity Strategy acknowledged the important role that private sector plays in the fight against cybercrime and to enhance cybersecurity.[209] [EQ16]

Despite the lack of related provisions in the Framework Decision, a number of public-private cooperation initiatives at national level have emerged, with the following **characteristics:**

- Most have been developed in recent years.

[207] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
[208] This section is based on the evidence provided in section 4.2.4 of the Study " Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combatting fraud in and counterfeiting of non-cash means of payment"
[209] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013

- Mostly involve only national stakeholders.
- The UK leads in terms of public-private co-operation.
- Most focus on cybercrime in general rather than on non-cash payment fraud only.
- Most involve financial institutions and law enforcement.
- They cover both reaction and prevention.
- When cooperating for prevention, they often organise raising awareness campaigns and deploy ad-hoc training.
- They contribute to investigation and prosecution by facilitating the exchange of information between the private sector and law enforcement, enhancing relationships and raising awareness that helps increase the prioritisation of these crimes.
- Most are highly formalised, with defined structures, and having continuous and ongoing activities.

Successful public-private cooperation typically:

- Involves a diversified set of private actors, so that they can provide a full picture of the phenomenon, since the information is usually spread among several stakeholders.
- Works in a formalised and structured way.
- Allows multilateral exchanges of information, not only between public and private actors, but also between private actors.
- Clearly communicates to the private sector the benefits they might perceive from co-operation.

The main **obstacles** that prevent public-private cooperation from reaching its full potential relate to **information sharing**, both domestically and cross-border:

- Lack of clarity on the requirements on private sector to collect information, which may affect the admissibility of evidence in court.
- Limited implementation by payment service providers of systems to monitor, handle and follow up on general security incidents (e.g. data breaches) and security-related customer compliance, and to notify the competent authorities (e.g. law enforcement). However, it shall be taken into account that the new data protection legislation contains rules on personal data breaches.

⇨ **Information sharing gaps** in **public-private cooperation** hamper prevention.

A specific case of information sharing is mandatory **reporting** to law enforcement, which contributes to gain a better understanding of the fraud case and therefore enables a better response and prevention. [EQ13, EQ14]

- Reporting obligations for payment services providers exist in the Payment Services Directive, in cases of major operational or security incidents, and in the fourth Anti

Money Laundering Directive,[210] for "obliged entities" (which include financial institutions), in case suspicious transactions are detected.

- A majority of Member States (16)[211] make it mandatory to report to law enforcement whenever there are suspicions raised with regard to the commission of an offence relating to payment instruments, computers and/or specifically adapted devices.
- **Under-reporting** is common in non-cash payment fraud, due to:
  - Poor information available to victims on the reporting systems in place, and the role of actors involved in their protection, which often differ from one Member State to another.
  - Reputational concerns of businesses, for example to expose publicly that they have been victim of data breaches. This is especially true in those counties that apply the principle of legality, i.e. all crimes that are reported must be also investigated.
  - The compensation to companies and individuals received by banks that make victims abandon the proceedings as soon as the reimbursement has been received.
  - Victims of fraud may blame themselves and/or fear that others will blame them for stupidity or even culpability.
  - Limitations in current reporting systems (e.g. lack of reporting mechanisms for internet crimes, lack of feedback to victims that report, lack of reporting categories,

⇨ **Under-reporting** to law enforcement due to constraints in **public-private cooperation** hampers effective investigations and prosecutions.

Efficiency

As specified in the section "Effectiveness" (above), it is very difficult to estimate any correlation between the Framework Decision and the dimension of crime and how/if it contributed to the formation of national criminal law frameworks. [EQ9; EQ18]

Many of the provisions of the Framework Decision have been supplemented by other (more effective) mechanisms: provisions on law enforcement cooperation (Article 12) becomes obsolete, if compared with the level of cooperation reached in the framework of the relevant Europol operational analysis project[212] and through the Payment Card Fraud priority under the

[210] Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

[211] AT, BG, CZ, DE, EE, EL, ES, FI, HR, IE, IT, LT, NL, PL, RO, SK

[212] "Terminal" operational analysis project in Europol's European Cybercrime Centre assists Member States and coordinates operations to tackle card-present and card-not-present fraud. All EU Member States participate in the "Terminal" operational analysis project, where also Interpol and law enforcement authorities from third countries

EU Policy Cycle. Provisions on extradition have today a limited added value, considering the possibility that Member States have to make use of European Arrest Warrants (see Section 6. Implementation state of play, above).

When looking at areas that are not covered by the Framework Decision, such as public-private cooperation, the success of the existing forms of cooperation[213] and the strong support from all parties to step up their commitment does not appear to be matched by appropriate provisions to facilitate information sharing and enhance reporting (see "Effectiveness", above). [EQ13, EQ14, EQ15]

Bearing in mind that the analysis is hampered by the difficulties outlined above, it is very difficult to establish the level of costs brought about by the implementation of the Framework Decision and even estimates are impossible, as it is unclear to which extent the Framework Decision is the underlying cause for new national legislation (see also "EU added value", below). Equally, benefits are unclear.

Coherence

Some issues have been identified as regards to the coherence of the Framework Decision with other relevant EU legislative acts. [EQ16]

1) Payment Service Directive (PSD2)[214] and the e-Money Directive:[215] definition of "payment instrument"
   The definition of payment instrument contained in the PSD2 covers non-corporeal payment instruments and in particular e-money. This definition includes most of the main non-cash means of payment, aside from those that are not personalised (e.g. some kinds of coupons) and those that do not initiate a payment order (e.g. fidelity/loyalty cards or virtual currencies).

   Thus, the PSD definition covers technologies that grew in importance after 2001 such as virtual cards, e-money, and electronic wire transfers. The definition of payment

---

that have agreements with Europol participate: Australia, Canada, Norway, and USA (US Secret Service, US Postal Inspection Service, FBI).

[213] The Study " Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combatting fraud in and counterfeiting of non-cash means of payment" analysed a number of national public-private cooperation initiatives:

- France: FIA-NET, Phishing initiative, Groupement des Cartes Bancaires (CB), and French LEA.
- Germany: the German Cybercrime Competence Centre (G4C);
- Italy: the platform OF2CEN, CertFin;
- The Netherlands: ECTF (Electronic Crime Task Force);
- Slovakia: Slovakian Banking Association Commission for security of payment cards;
- The UK: the Dedicated Card and Payment Crime Unit (DCPCU), Cyber information Security Partnership (CiSP), Action Fraud, Financial Fraud Action, National Cyber Security Center (NCSC).

[214] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

[215] Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of electronic money institutions amending Directives 2005/60/EC and repealing Directive 2000/46/EC

instrument has been further developed also through the E-money Directive 2009/110/EC that firstly provided the definition of e-money.

2) Directive on Attacks against information systems:[216] offences, definitions, penalties and jurisdiction
   - Directive 2013/40/EU on Attacks against Information Systems criminalises forms of conduct that are relevant to non-cash payment fraud and preparatory acts (such as theft of personal data), illegal interception of computer data, and attacks to information systems. However, Directive 2013/40 does not cover the possession, sale, making available of stolen data, which is relevant when considering preparatory acts for non-cash payment fraud.
   - The Directive on attacks against information systems replaces the notion of "computer system" included in the Framework Decision with the broader notion of "information system" and clarifies it, thus including systems which are not computer-based (and which are at the basis of most of the emerging forms of value transfers).
   - Directive 2013/40/EU provides mandatory minimum levels of maximum penalties, which the Framework Decision does not include. Experts (in the framework of the dedicated meetings organised by the Commission to gather input) indicated Directive 2013/40/EU as a possible source of inspiration in this area, if the Framework Decision was to be revised.
   - With regard to criteria to establish national jurisdiction, Directive 2013/40/EU provides for clearer criteria than those included in the Framework Decision. Again, Experts (in the framework of the dedicated meetings organised by the Commission to gather input) indicated Directive 2013/40/EU as a possible source of inspiration in this area, if the Framework Decision was to be revised.

3) European Arrest Warrant:[217] extradition

As presented in section 6, The European Arrest Warrant as lex posterior partially made redundant the provisions above, by setting conditions for compulsory extradition for offences covered by the Framework Decision (e.g. specifically “fraud, including that affecting the financial interests of the European Communities”, “forgery of means of payment”, “computer-related crime”, “participation in a criminal organisation”) when they are punished by a certain level of penalties.

EU added value

The Framework Decision added value [EQ17; EQ18] by setting a common criminal law framework of reference for Member States, even though this is also the result of the co-existence of other relevant EU legislation.

[216] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[217] 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision

The Framework Decision provides minimum definitions, principles, and criteria that created a certain degree of approximation of national legislative frameworks, therefore easing conditions for investigation and prosecutions. The Framework Decision added value by establishing a common framework to ease cross-border investigations and prosecutions in a context of an increasing international dimension of non-cash payment related fraud.

Even though most of the Member States have transposed the Framework Decision provisions, **it is difficult to establish whether the current level of harmonisation is the result of the Framework Decision only**. When looking at the provisions of the Framework Decision, there have been a number of relevant pieces of EU legislation that entered into force after 2001, which partially overlap and complement the scope of the Framework Decision, and that may have brought to changes in the national legislative frameworks.

In order to identify the effect (and therefore the added value) of the Framework Decision, the analysis carried out in the Study "Evaluation of the existing policy and legislative framework and preparation of impact assessment regarding possible options for a future EU initiative in combatting fraud in and counterfeiting of non-cash means of payment" (Section 4.5 of the Study)[218] focused on the dates of the last amendments of national legislation and compared them to the entry into force of other relevant EU legislation. However, the fact that a Member State has modified its legislation after the entry into force of the Framework Decision does not mean that this modification has produced effects. It is therefore difficult to conclude on added value on that basis.

Overall, only for few Member States it is possible to state that the Framework Decision had an added value, while for the majority of Member States the added value is uncertain, and for some the Framework Decision did not bring added value since their national legislative frameworks already integrated Framework Decision provisions. The Framework Decision added value appears today to be reduced by the coexistence of other and more relevant EU/international legislation. This is further confirmed by the fact that stakeholders involved in the study hardly recall the Framework Decision and make reference today to other and more recent EU level legislation.

While the Framework Decision contributed, at least to some extent, to the progressive harmonisation of national criminal law frameworks, it brought limited add value to the cooperation and the exchange of information needed to improve cross-border investigations and prosecutions. Member States still face some operational difficulties and cross-border investigations and prosecutions are sometimes hindered by a limited exchange of information, by different application of data protection legislation or by complex and lengthy procedures. Representatives from public and private sectors launched autonomously a number of initiatives and partnerships that remain essentially national, to address these obstacles. This highlights an area for further improvement.

[218] Study available in the EU Bookshop.

To conclude, the Framework Decision contributed to creating a common criminal law framework for EU Member States. However, the current level of harmonisation does not seem to be enough to adequately support cross-border investigations and prosecutions which are hindered by some operational concerns that are not uniformly addressed.

8. Conclusions

As described in annex 4., where the methodology is outlined, the evaluation of the Framework Decision and of the policy context has limitations in terms of the analysis of the transposition of the Framework Decision and the assessment of its impact (Lack of data on prosecutions and investigations, limited statistics allowing for a quantification of crime, limits of the stakeholder consultations).

Overall, the Framework Decision is only partially relevant to the needs of stakeholders in the area of non-cash payment fraud. Specifically, the scope of the Framework Decision is not fully relevant in view of recent technological developments, and provisions on cross-border cooperation and exchange of information do not seem to be aligned with the increasing international dimension of crime.

- Scope of the Framework Decision: the Framework Decision falls short in addressing fraud committed against new forms of payments (such as virtual payment cards, mobile money, virtual currencies), which are increasingly targeted by fraudsters, especially as regards to preparatory acts.
- In general, member States adopted wider definitions of payment instruments. However, some experts have reported challenges due to the dual nature of virtual currencies as computer data and monetary value. Virtual currencies are the main payment instrument which still falls outside the scope of existing legislative measures (both EU and national).
- Offences: the Framework Decision does not cover conduct that is preparatory and supportive to non-cash payment fraud without resulting directly in a transfer of money or monetary value. Many Member States went beyond the Framework Decision and adopted provisions to cover additional behaviours (e.g. social engineering or identity theft). The Directive on Attack against information systems partially remediated this, by including offences relating to computers and illegal interception of data. However, that fails to cover a number of preparatory acts (e.g. possession, sale of stolen credentials)

Assessment of achievement of strategic objective 1: *The Framework Decision appears to fall short in ensuring that conduct which are relevant for fraud and counterfeiting of non-cash means of payment are recognised as criminal offences*.

- Sanctions: the Framework Decision did not bring about a satisfactory level of approximation of sanctions across Member States. This is inconsistent with other relevant EU legislation, may have a negative impact on judicial cooperation and leaves the door open to forum shopping.

Assessment of achievement of strategic objective 2: *The Framework Decision appears to fall short in ensuring a satisfactory level of approximation of sanctions, as the level of sanctions is questionably effective in some Member States.*

- Cross-border cooperation: the high level guidance provided by the Framework Decision is not specific enough to meet the needs of stakeholders involved in cross-border investigations and prosecutions. Representatives from LEAs expressed the need for more measures of mutual assistance between Member States, and most of them considered the current level of cooperation only partly satisfactory with areas for potential improvement.
- Exchange of information: representatives from LEAs have identified obstacles in terms of procedures for the transmission of evidence, and limitations brought by differences in the current national data protection laws that are not currently addressed by the Framework Decision.
- Jurisdiction: issues were identified, as regards to possible negative conflicts of jurisdiction (i.e. cases where no Member State is able to claim jurisdiction)

Assessment of achievement of strategic objective 3: *The Framework Decision appears to fall short in ensuring a satisfactory level of cross-border cooperation and exchange of information.*

Additional contextual needs relating to non-cash payment fraud also affect the overall relevance of the current legal framework: data protection, reporting to LEAs, cooperation between the private and the public sectors and victims' rights:

- Current fragmentation in the implementation or limited scope of EU data protection rules created legal uncertainty for the cooperation between Member States and also between public and private sector representatives, especially within cross-border cases.
- Reporting to LEAs is currently not an obligation in all Member States and there are different practices and different focus among Member States; underreporting remains an issue.
- Considering the fragmentation of relevant information among actors affected by non-cash payment fraud, the creation of public-private cooperation initiatives is generally considered important. Initiatives analysed proved to have positively contributed to the improvement of investigations and to the design of preventive and repressive measures.
- Additional needs were raised with regard to some victims' rights which appear to be not adequately covered, and namely: psychological support, the right to recover losses, and the right to information.

It has been impossible to calculate costs and benefits linked to the Framework Decision, given the lack of relevant data and the impossibility to understand to which extent the Framework Decision is the underlying cause for new national legislation: many of the provisions of the Framework Decision have been supplemented by other (more effective) mechanism.

Some issues have been identified as regards to the coherence of the Framework Decision with other relevant EU legislative acts, such as the Payment Service Directive (PSD),[219] the Directive on Attacks against information systems[220] and the European Arrest Warrant:[221]

To conclude, the Framework Decision contributed to creating a common criminal law framework for EU Member States. However, the current level of harmonisation does not seem to be enough to adequately support cross-border investigations and prosecutions which are hindered by some operational concerns that are not uniformly addressed.

As a whole, the Framework Decision does not appear to have fully met its objectives.

In summary, the issues detected in the evaluation of the policy/legal framework are the following:

1. **Some crimes cannot be effectively investigated and prosecuted under the current legal framework.**
2. **Some crimes cannot be effectively investigated and prosecuted due to operational obstacles.**
3. **Criminals take advantage of gaps in prevention to commit fraud.**

These can be broken down in the following list of specific issues, linked to the **policy/legal framework** in place, as well as to the way the **policy/legal framework is implemented:**

Problems linked to the **policy/legal framework**:

a. Certain crimes cannot be prosecuted effectively because offences committed with certain payment instruments (in particular **non-corporeal**) are criminalised differently in Member States or not criminalised.

b. **Preparatory acts** for non-cash payment fraud cannot be prosecuted effectively because they are criminalised differently in Member States or not criminalised.

c. Deficiencies in allocating **jurisdiction** can hinder effective cross-border investigation and prosecution**.**

d. Under-reporting to law enforcement due to constraints in **public-private cooperation** hampers effective investigations and prosecutions.

[219] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

[220] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[221] 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision

e. **Information sharing gaps** in **public-private cooperation** hamper prevention.

f. Criminals exploit the **lack of awareness** of victims.

Problems linked to the **implementation** of the **policy/legal framework**:

e. Cross-border investigations can be hampered because the same offences are sanctioned with different **levels of penalties** across Member States.

f. It can take too much time to provide information in **cross-border cooperation** requests, hampering investigation and prosecution.

ANNEX 6: GLOSSARY

Term	Definition
PAYMENT INSTRUMENTS	
Bill of exchange	A bill of exchange is a written order from one party (the drawer) to another (the drawee) instructing the drawee to pay a specified sum on demand or on a specified date to the drawer or to a third party specified by the drawer. It is widely used to finance trade and, when discounted with a financial institution, to obtain credit.[222]
Cheque	A cheque is a written order from one party (the drawer) to another (the drawee, normally a credit institution) requiring the drawee to pay a specified sum on demand to the drawer or to a third party specified by the drawer.[223]
Coupon	A coupon is a discount offer printed in newspapers or magazines, attached to a packaging, or mailed out. A consumer redeems a coupon by presenting it at the time of paying for the discounted product.[224]
Credit transfer/Wire transfer	A wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. *Money remittance* is a type of wire transfer and namely a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.[225]
Direct debit	Direct debit is a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.[226]
Electronic money (e-money)	Electronic money is an electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds

[222] European Central Bank,,. The Payment System,. Tom Kokkola, 2010, p 343.
[223] European Central Bank, The Payment System,. Tom Kokkola, 2010, p 34.
[224] Business Dictionary, retrieved in June 2017
[225] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;.
FATF and GAFI, FATF IX Special Recommendations, 2001.
[226] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, Article 4 (Definitions).

Term	Definition
	for the purpose of making payment transactions and which is accepted by a natural or legal person other than the e-money issuer.[227] E-money can be either hardware-based (i.e. stored on a device, typically a card)[228] or software-based (i.e. stored on a computer server).[229]
Eurocheque	A Eurocheque is the equivalent of a traveller's check issued in the Euro currency. The check must be issued by a European bank and can be cashed at banks that display the "European Union" crest. Security measures have been put in place to ensure that a holder can still retrieve the funds of a Eurocheque should it be lost or stolen. The Eurocheque is no longer issued, as of 2002.[230]
Fidelity/loyalty card	A loyalty card is a card offered by some stores to their customers on which the card owner can store points that can be converted into vouchers that provide discounts on products or services. Customers are awarded a set number of points when they shop at the store, depending on how much they spend.[231]
Meal voucher/Ticket restaurant	A meal voucher is a ticket given by an employer to an employee in addition to their wages, which can be exchanged for food in a restaurant.[232]
Mobile money	Mobile money is the provision of financial services through a mobile device. This broad definition encompasses a range of services, including payments (such as peer-to-peer transfers), finance (such as insurance products), and banking (such as account balance inquiries). In practice, a variety of means can be used such as sending text messages to transfer value or accessing bank account details via the mobile Internet. *Carrier billing* means making purchases that are charged to the customer's phone account.[233]
Payment cards	Credit cards: A credit card is a card that enables cardholders to make purchases and/or withdraw cash up to a prearranged credit limit. The credit granted may be either settled in full by the end of a specified period, or settled in part, with the balance taken as extended credit (on which interest is usually charged).[234] Debit card: A debit card is a card enabling its holders to make purchases and/or withdraw cash and have these transactions directly and immediately charged to their accounts, whether these are held with the card issuer or not.[235]

[227] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC;. Article 2 (, Definitions)..
[228] For instance, prepaid cards are included in this definition.
[229] European Central Bank, The Payment System,. Tom Kokkola, 2010, p 351.
[230] InvestorWords, 'Eurocheque', retrieved in June 2017.
[231] BBC, 'loyalty cards', retrieved in June 2017.
[232] InvestorWords, 'Luncheon voucher', retrieved in June 2017.
[233] Donovan, K., Mobile Money for Financial Inclusion. Information and Communications for Development, 2012; PC Mag, 'direct carrier billing', retrieved in June 2017.
[234] European Central Bank, The Payment System,. Tom Kokkola, 2010, p 348.
[235] European Central Bank, The Payment System,. Tom Kokkola, 2010, p 349.

Term	Definition
	Commercial card: A commercial card is a payment instrument used only for business expenses charged directly to the account of the undertaking or public sector entity or the self-employed natural person.[236] Fuel card: A fuel card is used as a payment card most commonly for diesel, petrol and lubricants at filling stations.[237]
Travellers' cheque	A travellers' cheque is a prepaid paper-based product issued in specific denominations for general-purpose use in business and personal travel. It does not specify any particular payee, is non-transferable once signed and can be converted into cash only by its specified owner. It is generally accepted by banks, with many large retailers and hotels (and some restaurants) doing likewise.[238]
Virtual currency	Virtual currency (e.g. Bitcoin) is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, it is a valid and legal offer of payment) in any jurisdiction[239]. It is neither issued nor guaranteed by any jurisdictions, and fulfils the above functions only by agreement within the community of users of the virtual currency.[240]
CRIMINAL OFFENCES	
Acting as a money mule	The term "acting as a money mule" indicates a person who transfers proceeds of crime between different countries. Money mules receive the proceeds into their account; they are then asked to withdraw them and wire the money to a different account, often overseas, keeping some of the money for themselves.[241] Sometimes they know the funds are crime proceeds; sometimes they are deceived into believing that the funds are genuine.
Carding websites	Carding websites are websites where bundles of credentials are sold in varying sizes. Prices depend inter alia on whether the card data are taken from corporate cards which might have higher limits and be verified less frequently; on the time that has elapsed since the data theft has taken place; and on the completeness of the data file (e.g. additional information on the card holder might enable higher prices).[242]
Data breach	A data breach is an incident in which sensitive, protected or confidential data have been potentially viewed, stolen or used by an individual unauthorised to do so.

[236] European Payments Council, 'Commercial cards', 2015. Retrieved in June 2017.
[237] UKFuelCards, 'payment cards', retrieved in June 2017.
[238] European Central Bank, The Payment System, Tom Kokkola, 2010, p 32.
[239] *Overview and Analysis of the Concept and Applications of Virtual Currencies*, JRC Technical report EUR28386 EN
[240] FATF, Virtual Currencies Key Definitions and Potential AML/CFT Risks, Financial Action Task, 2014, p 4.
[241] ActionFraudUK, 'money muling', retrieved in June 2017.
[242] European Commission, Inception Impact Assessment - Combatting Fraud and Counterfeiting of Non-Cash Means of Payment, 2016, p 3.

Term	Definition
	Data breaches may involve personal data, such as for instance personal health information, trade secrets, or intellectual property.[243]
Eavesdropping (or sniffing)	Eavesdropping is the process of actively capturing datagram and packet information from a selected network. Sniffing acquires all network traffic regardless of where the packets are addressed.[244]
Malware	A malware is a malicious software that consists of programming, for example code or scripts, designed to disrupt the performance of PCs, laptops, handheld devices, and so on. Malware can also collect information or data from infected devices and pass them on to another device. Malware is often referred to as viruses, worms, trojan horses, spyware, dishonest adware, scareware, and crimeware.[245]
Man-in-the-middle	The term "man-in-the-middle" indicates an attack in which an attacker is able to read, insert, and modify messages between two users or systems. The attacker must be able to observe and intercept messages between the two victims.[246]
Skimming	Skimming occurs when a fraudster counterfeits a bank card by using a device to capture the card and account information embedded in the card's magnetic strip.[247]
Social engineering attacks	Social engineering attacks are attack vectors that heavily rely on human interaction and often involve tricking people into breaking normal security procedures. There are various techniques.[248] *Phishing* is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Most commonly, an email that appears to be from a well-known and trusted company is sent to a large list of email addresses. The email may direct the recipient to a spoofed Web page, where he or she is asked for personal information.[249] *Pharming* is a form of online fraud very similar to phishing as pharmers rely upon the same bogus websites and theft of confidential information. However, where phishing must entice a user to the website through 'bait' in the form of a phony email or link, pharming re-directs victims to the bogus site even if the victim has typed the correct web address.[250]

[243] TechTarget, 'Data Breach', retrieved in June 2017.
[244] Symantec, 'Sniffing', retrieved in June 2017.
[245] ActionFraudUK, 'Malware', retrieved in June 2017.
[246] Symantec, 'Man-in-the-middle', retrieved in June 2017.
[247] Financial Fraud Action UK, 'skimming', Action Fraud, p 44.
[248] TechTarget, 'Social Engineering', retrieved in June 2017;
Action Fraud, 'skimming', 2017, retrieved in June 2017.
[249] Action Fraud, 'Phishing', retrieved in June 2017.
[250] Symantec, 'Online fraud: pharming', retrieved in June 2017.

Term	Definition
	Smishing occurs when fraudsters obtain personal details of a victim by SMS text messages. SMS phishing uses phone text messages to deliver the bait to induce people to divulge their personal information.[251] A *romance scam* occurs when dating fraudsters form online relationships with individuals over weeks and months and then make a request for money when they feel they have established enough trust.[252] A *CEO attack* occurs when a fraudster purports to be a senior partner (or CEO equivalent) and contacts a member of staff with responsibility for authorising financial transfers, requesting payments to be made into bank accounts under the pretence of a highly sensitive or urgent transaction.[253]
OTHER	
Card-not-present transaction	CNP transactions are transactions based on payment cards with "MO/TO" (Mail Order/Telephone Order) commerce or e-commerce. In addition to these, card-not-present payments at the physical point of sale have emerged. Indeed, the capabilities of modern mobile telephones, or smartphones, also allow for the use of "remote payments", such as credit transfers at the physical point of sale.[254]
Card present transaction	Card-present transactions are transactions based on payment cards which can be made either in contact-mode (for which the card is inserted into the terminal) or as contactless payments (for which near-field communication technology is used and for which it is sufficient to bring the card close enough to the terminal without physical contact). For contactless payments, the "card" can also take the form of a mobile telephone,[255] or any object that can be equipped with a chip and an NFC-antenna.[256]
Darknet	Darknet (or dark web) refers to "encrypted online content that is not indexed on conventional search engines. The dark web is part of deep web, a wider collection of content that does not appear through regular Internet browsing. A specific browser like Tor is required to access dark web sites. The dark web holds anonymous message boards, online markets for drugs, exchanges for stolen financial and private data, and much more. Transactions in this hidden economy are often made in bitcoins and physical goods are shipped in a way to protect both the buyer and the seller from being tracked by law enforcement".[257]

[251] Action Fraud, 'SMSishing', retrieved in June 2017.
[252] Action Fraud, 'Romance scam', retrieved in June 2017.
[253] Action Fraud, 'CEO fraud', retrieved in June 2017.
[254] European Central Bank, Cards payments in Europe - a renewed focus on SEPA for cards, 2014, p 16.
[255] European Central Bank, Cards payments in Europe - a renewed focus on SEPA for cards, 2014, p 17 ('The capabilities of modern mobile telephones, or smartphones, also allow for the use of previous "remote payments", such as credit transfers at the physical point of sale. It also allows for making card-not-present payments at the physical point of sale. The latter raises specific concerns, as it circumvents the use of the chip on the physical card for card authentication').
[256] European Central Bank, Cards payments in Europe - a renewed focus on SEPA for cards, 2014, p 17.
[257] Investopedia, retrieved in June 2017.

Term	Definition
EMV standards	EMV® is a global standard for credit and debit payment cards based on chip card technology, taking its name from the card schemes Europay, MasterCard, and Visa, the original card schemes that developed it. The standard covers the processing of credit and debit card payments using a card that contains a microprocessor chip.[258]
Near Field Communication (NFC)	Near field communication is a form of contactless communication between devices like smartphones or tablets. When developing near field communication devices and new technology, NFC standards must be met. Standards exist to ensure all forms of near field communication technology can interact with other NFC compatible devices and will work with newer devices in the future. Two major specifications exist for NFC technology: ISO/IEC 14443 and ISO/IEC 18000-3. The first defines the identity cards used to store information, such as that found in NFC tags. The latter specifies the radio frequency identification communication used by NFC devices.[259]
Payment -service provider	Payment service providers are natural or legal persons providing one or several of the following services: (i) Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account; (ii) Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account; (iii) Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider; (iv) Execution of payment transactions where the funds are covered by a credit line for a payment service user; (v) Issuing of payment instruments and/or acquiring of payment transactions;(vi) Money remittance; (vii) Payment initiation services; (viii) Account information services. They can be credit institutions and e-money institutions including their branches located in the EU, post office giro institutions, payment institutions, the European Central Bank (ECB), national central banks, Member States or their regional or local authorities when not acting in their capacity as public authorities.[260]

[258] Level2Kernel, 'What is EMV Chip Card Technology?', retrieved in June 2017.
[259] NearFieldCommunication.org, retrieved in June 2017.
[260] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC; Article 4 (Definitions).