INCEPTION IMPACT ASSESSMENT			
TITLE OF THE INITIATIVE	Combatting Fraud and Counterfeiting of Non-Cash Means of Payment		
LEAD DG – RESPONSIBLE UNIT – AP NUMBER	DG MIGRATION AND HOME AFFAIRS – UNIT D2 ORGANISED CRIME - 2016/HOME/077	**DATE OF ROADMAP**	04/05/2016
LIKELY TYPE OF INITIATIVE	Legislative proposal		
INDICATIVE PLANNING	*http://ec.europa.eu/atwork/pdf/planned_commission_initiatives_2016.pdf*		
ADDITIONAL INFORMATION	-		

This Inception Impact Assessment is provided for information purposes only and can be subject to change. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.

A. Context, Subsidiarity Check and Objectives

Context

Concerns of users about online safety have risen in the last years, as the most recent Eurobarometer on Cyber Security shows. The vast majority of Internet users (85%) feel that the risk of becoming a victim of cybercrime is increasing. When using the Internet for online banking or shopping, 42% of users are worried about the security of online payments. Because of security concerns, 12% are less likely to bank online. 8% say they have already been a victim of credit card or banking fraud online and 7% say they have experienced identity theft.

These crimes create significant costs to the EU economy, as they result in a reluctance of users to fully engage with the digital economy. The Digital Single Market Strategy[1] aims to reinforce user confidence in the digital marketplace. Several initiatives are already aiming to set in place stronger preventive measures. The implementation of the revised Payment Services Directive (PSD2)[2] and the imminent adoption of the Directive on Network and Information Security (NIS Directive)[3] will lead to increased security of financial services systems and of payment services. The PSD2 contains a number of measures which will enhance the security requirements for electronic payments and will provide a legal and supervisory framework for emerging actors in the payment market. The NIS Directive 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. However, such preventive actions need to be complemented by effective measures to sanction criminal activity and to enable prosecution where prevention has failed.

In the European Agenda on Security[4] (EAS), the Commission committed to reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments. The EAS acknowledges that the present EU rules no longer reflect today's realities and insufficiently address new challenges and technological developments. President Juncker included improved rules on fraud in non-cash payments in his September 2015 Letter of Intent (priority #7: An Area of Justice and Fundamental Rights based on mutual trust) for delivery in 2016.

The current rules are based on Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment. While a full evaluation according to the Commission's Evaluation Guidelines remains to be performed in the framework of external study which will be contracted out in spring 2016 *(see also below under 'Consultation approach')*, other exercises have provided information about the state of implementation and the strengths and weaknesses of the current legal framework: two implementation reports were completed in 2004 and 2006;[5] relevant national provisions have also recently been analysed under the *Study on criminal sanction legislation and practice in representative Member States*.[6] Furthermore, operational

1 COM(2015) 192 final.
2 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 - OJ L 337, 23.12.2015, p. 35–127.
3 COM(2013) 48 final.
4 COM(2015) 185 final.
5 COM(2004) 346 final and COM(2006) 65 final.
6 http://www.ec.europa.eu/justice/criminal/document/files/sanctions_delivery_en.pdf.

action under the EU EMPACT Policy Cycle[7] has provided additional evidence as to the effectiveness of the existing rules.

In the area of criminal law, EU rules exist already in related areas, notably on attacks against information systems[8], on victims' rights[9] and on counterfeiting of the Euro[10]. The **directive on attacks against information systems** covers the attacks against infrastructure that are frequently committed as part of the preparations for a non-cash payment fraud, as for example in the case of a data theft of payment card credentials: the hacking into a system, the illicit interception of communications or other technical attacks fall under the scope of the directive. The **directive on victims' rights** sets minimum standards for Member States in dealing with victims, including their right to receive appropriate information, support and protection and ability to participate in criminal proceedings. The right to support also includes a right to receive advice relating to financial and practical issues arising from the crime (Art. 9) and a right to obtain a decision on compensation by the offender (Art. 16). The **directive on counterfeiting of the Euro** covers the counterfeiting of Euro and other currency notes and coins as well as related actions such as the creation of instruments for the production of false coins and notes or the import and export of counterfeit currency.

Issue

Non-cash payment frauds affect the trust of the public in digital services and undermine the strengthening of the digital single market. Fraudsters manage to adapt rapidly their *modi operandi* to evolving technologies and exploit legal loopholes and discrepancies, setting up transnational criminal networks, posing challenges to law enforcement.

Non-cash payments constitute an increasing share of overall payments. With the rising prevalence of e-commerce and other transactions at a distance, their importance for the economy is growing. Security at the Automatic Teller Machines and physical point of sale (POS) has continually improved with the introduction of standards such as chip-and-PIN technology (EMV[11]). The overall level of security applying to all Payment Service Providers for all electronic transactions and for access to the online banking environment will be further strengthened with new rules implementing the PSD2 and the NIS Directive. They are likely to impact both the level of fraud notably for card non present transactions and access to online banking and the types of fraud committed.

Frauds can take many forms.[12] Three examples may serve to illustrate some of the techniques currently used worldwide. **Skimming** is one of the most common forms of non-cash payment fraud: criminals copy the information stored on a payment card by means of a small device attached to an Automatic Teller Machine (ATM) – e.g. during a cash withdrawal – or to a physical point of sale (POS) device. In a typical **phishing** scheme, a user receives an email that purports to be from his or her bank and contains a link to an infected website designed to appear legitimate. This website asks for customers to divulge financial data, such as account credentials, login information, personal identification numbers (PIN), transaction authentication numbers (TAN) and credit card numbers. **Pharming** occurs when attackers hijack a bank's URL and manage to divert traffic to a site of their own that looks legitimate and similarly seeks to harvest credentials and other personal data.

The data harvested via these three methods and others can then be used in several forms: again, three examples of current practices may serve to illustrate the main uses. (1) Criminals can **create counterfeit payment cards** with the skimmed data and use those to pay in stores or withdraw cash at Automatic Teller

7 Created in 2010, the EMPACT Policy Cycle enables closer operational cooperation between EU Member States and select third countries on a set of priority areas in the fight against serious and organised crime. It brings together law enforcement agencies including Europol, the judiciary (Eurojust) and other relevant actors. For more information please see: https://www.europol.europa.eu/content/eu-policy-cycle-empact.

8 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, OJ L 218, 14.8.2013, p. 8–14.

9 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, OJ L 315, 14.11.2012, p. 57–73.

10 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, OJ L 151, 21.5.2014, p. 1–8.

11 EMV is a global standard for credit and debit payment cards based on chip card technology.

12 A helpful overview is provided at http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/.

Machines (see below for security measures seeking to address these issues). (2) They can **sell the data online** on so-called "carding sites"[13] where bundles of credentials are sold in varying sizes. Prices depend inter alia on whether the card data is 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). (3) Criminals can **use data** stolen or acquired on a carding site **to make online purchases** of goods and services. As the physical card is not required in this setting, it is also referred to as card-not-present fraud.

In 2013, **fraud using cards issued in the Single European Payment Area SEPA reached EUR 1.44 billion, representing a growth of 8% on the previous year**. The growth was driven by a 20.6% increase in card-not-present (CNP) fraud. Of the total fraud value, 66% of value resulted from CNP payments, 20% from point-of-sale (PoS) transactions and 14% from transactions at ATMs.[14] This results in a loss of trust in digital services. As mentioned before, because of concerns about frauds and other security risks, 12% of users in the EU are less likely to bank online and 13% have hesitation about shopping online. It also limits their willingness to engage with new products and services: 36% of users say that they only visit websites that they know and trust.[15] In economic terms, these are important lost opportunities for the digital single market.

Cross-border dimension

These crimes have a **significant cross-border dimension,** both within the EEA and frequently also beyond; the cases where just one country is affected are increasingly rare. A typical case may involve the skimming (copying) of card data in an EU country, the creation of a counterfeit card using that data, and the cashing out with the counterfeit card outside the EU, to circumvent the high security standards that have become the norm in the European Economic Area for Point-of-Sale (POS) card present transactions and Automatic Teller Machines cash withdrawals, such as EMV. Increasingly, these crimes are moving entirely to a virtual dimension due to the lack of suitability of card payments' security standards and processes (EMV) to the online world. As a result, stolen card credentials can be used to purchase goods or services online in the name of the unwitting card holder but for the benefit of the criminal. In the EEA however, under PSD2, authentication for remote electronic transactions implies a dynamic link to the amount and the recipient resulting in one-time authenticators which are specific to the transaction and cannot be reused. This is likely to reinforce the worldwide cross-border dimension of these crimes, and to lead to potential changes in the types of fraud attempted in the EEA.

Victimisation

Non-cash payment fraud typically directly affects **three entities**: (1) the financial services industry, (2) retail goods and services providers, and (3) individual consumers. A **financial services provider**, as issuer of a credit or other payment card or provider of account services, may bear the financial burden of a non-cash payment fraud committed against one of its customers except where the liability is passed on to the merchant. A **retail goods or services provider** can be the victim of the fraud committed by a criminal using fraudulently acquired payment (card) credentials, e.g. where 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. The **individual consumer** is affected by the use of his or her fraudulently acquired payment (card) data which can cause financial loss and expose the individual to negative credit ratings or other negative consequences of identity theft. Victims can be found in all parts of society. The general public suffers negative effects, such as intrusion in their privacy, loss of access to increasingly key payment functions and fraud crime attacks targeted at them directly.

According to statistics the **most rapid increase** in fraud on the Internet worldwide is reported by the **airline industry**, which is faced with fraudulent online purchases of flight tickets using compromised credit card data, often stolen through online data breaches. The airline industry faces significant losses as a result, estimated at EUR 1 billion.[16]

In terms of indirect consequences, credit card fraud was also highlighted as a key facilitator for other forms of serious crime; for example, fraudulently acquired airline tickets are used to transport victims of human trafficking or to smuggle drugs or persons.[17] Organised crime groups (OCGs) also operate fake travel agencies that sell last-minute tickets at steep discounts to more or (often) less unwitting customers and provide travel services for the purposes of the OCG itself to facilitate organisation of and participation in other crime.

Other stakeholders in this field include law enforcement and the judiciary, who are faced with significant

[13] There are often replete with tutorials for newcomers, tools and card data, as well as a feedback section allowing for vendor rating and quality control.

[14] *Fourth report on card fraud* – European Central Bank (July 2015) https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf.

[15] 2015 Special Eurobarometer 423 on Cybersecurity, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf, p. 33

[16] https://www.europol.europa.eu/content/global-action-against-online-air-ticket-fraudsters-sees-130-detained.

[17] https://www.europol.europa.eu/content/113-people-detained-and-70-arrested-action-day-tackling-airline-fraud.

challenges when investigating and prosecuting these crimes (see below for details), as well as civil society organisations such as victim support organisations and organisations dealing with data protection and privacy issues, who are concerned about the identity theft that frequently takes place as part of non-cash payment fraud.

A law enforcement response in need of improvement

While the abovementioned NIS directive and the revised Payment Services Directive will increase security of payment transactions, it might reinforce the worldwide cross-border dimension of these crimes, or lead to potential changes in methods and types of fraud attempted in the EEA. Although not comparable to the enhancement of legal security requirements on all Payment Service Providers for all electronic transactions and for access to the online banking environment under PSD2, in the past, the widespread adoption of the chip-and-PIN standard by the industry within the EEA temporarily lowered payment card fraud overall as it increased security for card present transactions but then criminals moved their cashing-out operations to the countries outside the European Economic Area where no such standard was implemented.

Furthermore, the protection of citizens against such crimes and their investigation and prosecution has proven difficult for a number of reasons:

- Certain behaviour, while harmful to society, is **not criminalized as it constitutes a new modus operandi** not yet covered by present-day rules. For example, the use of card payment credentials online (so-called card-not-present fraud) is not always explicitly covered, nor is the trade in card data as many Member States only cover the trade in physical fruits of illicit activity.[18] Cross-cutting enabling factors such as banking malwares and money mules are also not considered. At the same time, new forms of fraud, such as social engineering, are increasing and the enhancement of security requirements under PSD2 could reinforce this trend. The underlying cause of this problem is that current EU rules on fraud and counterfeiting of non-cash means of payment are **insufficiently technology neutral**: for example, they only cover physical (corporeal) payment instruments, i.e. a plastic card or a cheque.
- Furthermore, **investigations are often limited** to the acts committed within the country, if not for legal, then for practical reasons. Even where criminality could be established, non-cash payment fraud offenses now **frequently go at least partially unsanctioned**, leading to low overall criminal sanctions and a swift release of the perpetrators – and therefore low deterrence.[19] For example, an operation where data was stolen in country A and then used to withdraw funds in country B may result in a conviction in country A only for the data theft itself. The underlying cause of this problem lies in the challenge of pursuing an extraterritorial investigation. Where the evidence is located outside the state leading the investigation, obtaining it requires lengthy and time-consuming procedures.
- Law enforcement is **limited in its use of investigative tools**. One driver of this problem lies in lower levels of sanctions as use of investigative tools is often restricted to crimes of a certain severity, as reflected in sanctions applied.
- The fight against non-cash payment fraud is **not a priority** in many Member States. This is in part due to its nature as a high-volume, low individual impact crime as criminals often defraud many victims of smaller sums, and in part due to low sanction levels which have a strong influence on national priority setting.
- **Cooperation between law enforcement agencies of different Member States** can be challenging, due to the divergence in national laws as certain behaviour may be criminalized in one Member State but not in another, or may be sanctioned at very different levels.
- **Victims** may suffer from long-term impacts of identity theft, such as negative entries in their credit history. The underlying cause is the **lack of well-established victims' rights** when faced with identity theft. While the financial damage of a fraudulent payment card transaction is usually covered by the issuing bank, the underlying case of identity theft is insufficiently addressed: if the victim refuses to pay bills incurred by the criminal, this can lead to a negative credit history that has proven difficult to rectify in many instances.[20]
- There is **little reliable and detailed information** both on individual cases and on the overall scale and impact of non-cash payment fraud available to law enforcement. The private sector plays a key role here

[18] See, e.g., the recent legislation in Germany as an example of new criminalisation of trade in stolen data: http://dip21.bundestag.de/dip21/btd/18/050/1805088.pdf - new § 202d StGB, "Datenhehlerei" [Dealing in illicitly acquired data].

[19] Europol Situation Report Payment Card Fraud 2013, https://www.europol.europa.eu/content/situation-report-payment-card-fraud-european-union.

[20] http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf.

because close to all infrastructure affected by the crimes is privately owned; cooperation is therefore of the essence. The underlying driver of this problem lies in the lack of incentives and well-established reporting channels. Reporting channels between the financial services industry and their regulators are well-established and will be further strengthened under PSD2. However, the PSD 2 has not been implemented yet, and there is at this stage little evidence of up-to-date information on frauds and other crimes being passed on to law enforcement with the necessary swiftness to enable effective law enforcement action. The incentive for victims – who may be reimbursed by their banks – to report crimes to police is low, and the financial services industry – in the absence of established channels and procedures – may face significant legal uncertainty when considering to proactively report.

- Moreover, the knowledge about the size and nature of criminal activities related to fraud and counterfeiting of non-cash means of payment and the effectiveness of the law enforcement response is still partial and fragmented, in the absence of **comparable statistics**.

Subsidiarity check

In accordance with Article 67 of the Treaty on the European Union, the Union's objective shall be to provide citizens with a high level of safety. This objective shall be achieved by preventing and combating crime. Action of the Union in this field should be taken only if and in so far as this objective cannot be sufficiently achieved by the Member States and can be better achieved by the Union.

The EU has the competence to adopt common minimum rules on the definition of criminal offences and sanctions if they are essential for ensuring the effectiveness of a harmonised EU policy 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. Counterfeiting of means of payment is explicitly mentioned in Article 83 (1) TFEU as such an area of particularly serious crime.

Acting at EU level has an added value as the cross-border dimension of these offences is very important. While the cross-border activity of e-commerce consumers may still be low,[21] non-cash payment fraud is a problem which only rarely can be fought in a mere national context. They affect all Member States, and there is evidence that a considerable proportion involves activities from one Member State to another or beyond.

The transnational nature of non-cash payment fraud reflects the transnational structure of the criminal organisations typically perpetrating such crimes on a larger scale. Organised crime groups (OCGs) now frequently have an international setup and are regularly active across several states.[22] A criminal structure involved in payment fraud is usually very complex, highly specialised and hierarchical, with specific roles assigned to each member of the OCG. These OCGs make significant investments into the creation of malicious software ("malware"), which is then deployed as widely as possible with no regard for national boundaries. Europol has coordinated several cross-border investigations against worldwide criminal networks affecting the EU;[23] to cite an example, one major recent initiative addressed malware known as GameOverZeus which had infected more than one million computers around the globe and caused millions of Euros in damages.[24] These crimes create situations where the victim, the criminal and the evidence are all under different jurisdictions within the EU and beyond. As a result, it is impossible for single countries to effectively counter these criminal activities at a national level.

The objective of effectively combating such crimes therefore cannot be sufficiently achieved by Member States acting alone or in an uncoordinated way. This was acknowledged by the already existing EU legislation on combating fraud and counterfeiting of non-cash means of payment. It is also reflected by the concerted action taken by Member States in this field, with the creation of a dedicated Europol Focal Point on payment fraud and the EMPACT Policy Cycle priority on operational cooperation against non-cash payment fraud.

If the EU was not acting, Member States would have to update their national laws to respond to new and emerging challenges with the likely consequence of further fragmentation

However, the existing EU legislation on combating fraud and counterfeiting of non-cash means of payment has become outdated as it focuses on physical credit cards and cheques. As outlined above, payment card data and potentially other payment credentials in virtual form, such as login and password for an online account, are currently valuable to criminals although the enhancement of security requirements under PSD2 will impact this. All these aspects are not covered by the 2001 EU framework decision and furthermore are not fully covered by national laws either as those are also in need to be updated to reflect new criminal methods. As a result, current

21 COM(2011) 942.

22 Europol Serious and Organised Crime Threat Assessment 2013, p. 32.

23 Europol Situation Report Payment Card Fraud 2013, https://www.europol.europa.eu/content/situation-report-payment-card-fraud-european-union.

24 https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

rules fail to take into account technological developments.

Another value added in common definitions across the EU and a common understanding on minimum levels of sanctions would be to facilitate cooperation with third countries considering the important international dimension of most non-cash payment fraud crimes which also cross the external borders of the EU at some point in the operation. It may also inspire effective legislative solutions in third countries, as these could rely on the application of one and the same definition of what is criminalized – at a minimum – across the EU.

Main policy objectives

The general objective of the initiative is to address new and evolving forms of non-cash payment fraud, decreasing its occurrence and deterring potential criminal activity thereby reinforcing the trust of consumers in the digital single market and strengthening data protection more effectively.

Its specific objectives are:

- Enabling law enforcement investigations against new forms of non-cash payment fraud;
    - Enabling stronger cooperation between Member States' law enforcement agencies and with Europol on non-cash payment fraud;
    - Enabling stronger cooperation between the public and the private sectors;
- Empowering the private sector to better protect itself and its consumers against non-cash payment fraud;
- Strengthening the rights of victims of non-cash payment fraud.

B. Option Mapping

Policy options to be further assessed include:

1. A baseline scenario with no change;
2. Improved implementation and enforcement of the existing rules (see below for further details);
3. A legislative framework building on the provisions of the Framework Decision and including provisions extending to additional substantive criminal law rules addressing newer forms of non-cash payment fraud as well as setting minimum levels of maximum sanctions;
4. A legislative framework covering the substantive provisions outlined under Option 3. and extending to certain procedural law provisions, such as adapting the rules on jurisdiction for injunctions for cooperation/evidence to enable investigators and prosecutors to obtain the required data for their case;
5. A legislative framework addressing obstacles to the establishment of Public-Private Partnerships, enabling closer operational cooperation between law enforcement agencies across Member States (e.g. through the creation of dedicated points of contact) and providing for the collection of statistics on the investigation and prosecution of offences in this field. This could be envisaged in conjunction with the rules outlined under Options 3. or 4. above.
6. A self-regulatory framework for public-private cooperation between relevant actors from the financial services industry, law enforcement and other stakeholders, in conjunction with Option 2 or a legislative framework outlined above.

Baseline scenario – no EU policy change

Taking no action at EU level would leave the current legal system untouched in its current form, at least as far as criminal law measures specifically addressing non-cash payment fraud are concerned. There have been since 2001 significant policy changes in related areas, notably on preventive measures linked to increased resilience and greater security of payment systems, and on victims' rights through the victims' directive. Furthermore, certain parts of the activities of non-cash payment fraud offenders (e.g. hacking into a retailer's data storage to steal customers' payment credentials) are also covered under the directive on attacks against information systems. As a result, parts of the problems outlined above are better addressed now than they were a few years ago.

However, while the NIS directive and the revised Payment Services Directive will increase the security of financial transactions, it might reinforce the worldwide cross-border dimension of these crimes, or lead to potential changes in criminal methods and in the types of fraud attempted in the EEA. In the absence of an initiative addressing current and possible future criminal methods, the problems related to the lack of effective measures to sanction criminal activity and to enable prosecution where prevention has failed as outlined above are therefore likely to persist or increase.

Options of improving implementation and enforcement of existing legislation or doing less/simplifying existing legislation

Non legislative measures could be considered to support and improve the implementation and enforcement of the main piece of existing EU legislation in this field – the Framework Decision**.** They could include activities undertaken with the Member States to ensure that the provisions of the Framework Decision are utilized to their fullest, and/or the publication of a third implementation report alongside a guidebook explaining the legislative framework in each Member State to law enforcement and other stakeholders, in order to facilitate cooperation. It could also include a self-regulatory public-private partnership for better exchange of information between the public and private sectors (please see below under **Alternative policy instruments** for more details).

This option could improve the implementation of the existing provisions, possibly leading to reinforced investigations and prosecutions in the relevant areas of non-cash payment fraud, notably the creation and abuse of fraudulent cards and cheques. On the other hand, while the two implementation reports[25] show that there may indeed be room to improve implementation, this option would not address new technological and criminal developments and therefore might not cover a significant portion of criminal activity and harm to victims in this field.

Alternative policy approaches

Another approach is the adoption of a new legislative instrument in the area of criminal law, based on Art. 83(1) TFEU, and which could notably, but not only, build on the provisions of the 2001 Framework Decision.

There are different possible actions which should be further assessed:

- In addition to the current provisions of the 2001 Framework Decision, include **substantive criminal law rules addressing newer forms of non-cash payment fraud** as well as **setting minimum levels of maximum sanctions**. This would involve extending the scope of the current 2001 Framework Decision, with a view to make the legislation technology-neutral and fit for technological developments such as payment fraud on the internet and fraud related to other payment channels and new forms of fraud (e.g. social engineering). This could include measures against trafficking of credentials and the creation and operation of carding websites for the purposes of such transactions, and against certain preparatory actions closely linked to non-cash payment fraud, such as identity theft. It may also be appropriate to analyse whether any measures can be taken in this context to better address cross-cutting enabling factors such as banking malwares and money mules. Furthermore, specific aggravating circumstances (e.g. organised crime) could be identified that might give rise to the application of higher sanctions.
- Adopt certain **procedural law provisions**, such as to adapt the rules on **jurisdiction** both on substantive law and on procedural law. For the application of substantive law, this could notably include granting jurisdiction to a given Member State for the conduct of perpetrators who are citizens or permanent residents of that Member State regardless of where they acted and regardless of whether or not the conduct is criminalized in the destination state. While the 2001 Framework Decision contains rules covering some aspects, the rules have a very narrow scope of application with many exceptions. In procedural terms, this option could also include rules to complement the European Investigation Order[26] to enable timely access to electronic evidence, allowing investigators and prosecutors to obtain the required data for their case. It could furthermore include measures to strengthen victims' rights such as procedural safeguards for the rectification of negative entries in victims' credit history.
- Consider provisions **to address obstacles to the establishment of Public-Private Partnerships** (e.g. creating a framework allowing sharing of personal information where required, subject to the necessary safeguards, and addressing liability issues that may arise for the parties to the partnership as a result of the cooperation); furthering operational cooperation between law enforcement agencies across Member States (e.g. through the creation of dedicated points of contact) and collecting statistics on the investigation and prosecution of offences in this field.

Other measures/options may be defined in the course of the impact assessment work and/or as a result of the consultation process.

A mixture of different elements contained in different types of options could be retained as the preferable way forward to address the identified problems (for instance legislative provisions related to the establishment of

[25] COM(2004) 346 final and COM(2006) 65 final.

[26] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

Public-Private Partnerships, operational cooperation and statistical data collection, could be complementary to non-legislative measures to improve the implementation and enforcement of the existing legislation).

Alternative policy instruments

As mentioned above, the exchange of information between the financial sector and law enforcement, could be promoted through self-regulating public-private partnership. Such public-private partnerships already exist in a number of Member States and can rely on existing legislation governing data protection and other issues but no dedicated framework governing other questions of such cooperation, like liability, how to treat information shared, etc.

Self-regulation could be envisaged at the national or at the EU level (or could include further countries). If created at the national level, a self-regulatory model allows for national solutions that take account of e.g. specific regulatory requirements in a Member State. An obvious advantage for participants might be that they themselves define the framework for their cooperation and determine which rules to apply. It would also mean that the existing public-private partnerships would not face any changes that might affect how they operate. A drawback – also from the perspective of the participants – could be the lack of legal certainty that might come with an entirely self-regulatory solution.

Alternative/differentiated scope

As the principal elements of this initiative concern criminal law, it is impossible to envisage an alternative or differentiated scope.

Options that take account of new technological developments

The purpose of this initiative is to take account of new technological developments and to create rules that will be sufficiently technology-neutral to withstand the test of time and be effective also in light of further changes in the ways in which criminals operate in this area.

Preliminary proportionality check

The chosen option should be proportional in view of the policy goals and not go beyond what is necessary to meet these objectives. A definitive assessment is not possible on the basis of current information as the detailed evaluation of existing policy and the detailed impact assessment including the preparatory study still remain to be carried out. The check performed here is therefore of preliminary nature and conclusions may change depending on the outcomes of the evaluation and impact assessment exercises.

All legislative options considered could lead to a strengthened protection of personal data, albeit to different extents. Effective enforcement of clear rules on data theft and trade and proportionate criminal sanctions would complement the security and data breach rules to create better data protection. The deterrent effect of more successful investigations and proportionate sanctions could further enhance the prevention of identity theft and protection of personal data. At the same time information gathering and sharing (e.g. in public-private cooperation) required to fight crime can also affect the privacy rights of the victims or third parties where their personal data is concerned. Given the very wide definition of personal data which can include IP addresses, close to all information shared would constitute personal data. Therefore the right to data protection of the victim and other affected parties would need to be weighed against their interests to be protected from crime and to see crimes that affect them appropriately investigated, and against the general societal interest in ensuring effective law enforcement and prosecution of crimes. For this balance, the appropriate safeguards for any sharing of personal data would need to be identified and put in place.

All options will have to be carefully weighed – as does any criminal law measure – and undergo a comprehensive fundamental rights assessment. Any action of the Union in this field must respect fundamental rights and observe the principles recognised in particular by the Charter of Fundamental Rights of the European Union (EU Charter) and the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and notably the protection of personal data and the right to freedom of expression, the right to a fair trial, presumption of innocence and the right of defence as well as the principles of legality and proportionality of criminal offences. Member States, when implementing Union law, must do so in accordance with these rights and principles.

The new provisions would ensure the simplification of the legal framework and would facilitate the cooperation between Member States. Furthermore, the scope of the legislative action taken by the EU would be limited to those areas where Member States have not yet adopted rules that already reach the objectives set out here. The definitions to be set out will be based on the Framework Decision for some offenses, therefore comprising

rules that the Member States have already put in place. For new definitions to be introduced, due attention will be paid to existing rules and definitions where those exist in Member States already to avoid unnecessary changes. Finally, the definitions to be set out in the directive constitute minimum definitions only, leaving it up to Member States to define a wider scope for the application of criminal sanctions.

All legislative options would entail the introduction of minimum levels of maximum sanctions. This is necessary to ensure a coherent treatment across Member States, as the level of penalties has a strong effect both on the possible investigatory measures and on the priority given to the investigation of such crimes. At the same time, given that the levels imposed by a directive would only set a minimum for the maximum penalty, they leave it entirely up to Member States to set lower minimum sanctions or to impose higher maximum sanctions and hence preserve all flexibility needed to adapt sanctions to the national circumstances or preferences.

The form of Union action considered should be as simple as possible in limiting itself to central aspects of substantive and procedural criminal law and should minimize complications in implementation and enforcement.

C. Data Collection and Better Regulation Instruments

Data collection

A significant amount of data on the current situation and possible shortcomings is available. There have been two implementation reports on the Framework Decision, of 2004 and 2006,[27] four reports on card fraud by the European Central Bank (ECB),[28] as well as a number of studies developed by Europol[29] and EU projects[30] on the current system. A number of national studies into cybercrime and non-cash payment fraud more specifically have been conducted.[31] Furthermore, the Commission has contracted out an in-depth study on identity theft in 2012-2013 which can provide data on the impact of identity theft, e.g. for trade in credentials.

The ongoing GENVAL Mutual Evaluation Process on cybercrime, which produces detailed reports on each country's legislative framework, best practice and obstacles, also contains valuable information on how countries deal with non-cash payment fraud in all of its forms.

Experience from the European Cybercrime Centre[32] and national law enforcement on cross-border cases is a further valuable source that will help identify cases where current rules fail to adequately address criminal activities, which can serve as test cases for legislative options. These cases will be collected on an ongoing basis through bilateral contacts with the European Cybercrime Centre and through regular meetings with the Member States participating in the EMPACT Priority on Non-Cash Payment Fraud, which meet four times a year in the presence of the Commission.

Further information and data, both about the functioning of the current legislative framework to enable a comprehensive evaluation, and about the possible impacts of a new legislative proposal, are required to complement the existing information.

A comprehensive data collection exercise will be conducted, with an external study, a public consultation and expert groups as well as targeted consultation of stakeholders. The study is expected to be launched in Spring 2016, while the public consultation and meetings of expert groups should take place during the second half of 2016.

Consultation approach

The consultation will consist of three parts: (1) an external study; (2) a public consultation; and (3) targeted consultation of key stakeholders (financial services industry, select retail services providers, civil society including victims' organisations, and law enforcement and the judiciary) through questionnaires, workshops and expert meetings.

(1) The external study will perform two tasks: it will on the one hand provide a full ex post evaluation of the existing legal framework, namely the Council Framework Decision 2001/413/JHA, building on the implementation reports, updating the relevant information and performing a more thorough evaluation of achievements and shortcomings and, on the other hand, assess the scale of the problem and evaluate

27 COM(2004) 346 final and COM(2006) 65 final.

28 See https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf for the latest report.

29 https://www.europol.europa.eu/content/situation-report-payment-card-fraud-european-union.

30 See, e.g. http://ecrime-project.eu/; http://www.bristol.ac.uk/law/news/2015/project-skynet.html.

31 See, e.g., the UK House of Commons Home Affairs Committee 2013 inquiry into e-crime, report available at http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/inquiries/parliament-2010/e-crime/.

32 https://www.europol.europa.eu/ec3.

the policy options identified above. The first part should provide an evaluation report; the second part will feed into the Commission's full impact assessment. The Commission Impact Assessment work should start in 2016.

(2) The public consultation should be launched in spring 2016 and should consist of a public questionnaire using EU Survey, assessing public perception of the scale of the problem and responses to possible solutions at EU level. The launch of stakeholder consultations related to this initiative will be announced in the consultation planning that can be found at http://ec.europa.eu/yourvoice/consultations/docs/planned-consultations_en.pdf.

Targeted consultation of key stakeholders should also begin in June 2016 and conclude by November 2016, in the form of workshops and expert meetings. This work will be supported by the Commission's Joint Research Centre and by the EMPACT Policy Cycle Priority on Non-Cash Payment Fraud.

Consultation of the **financial services sector** will focus on their role as co-victims of the crimes, the scale of the problem in terms of financial damages (e.g. customer reimbursement for fraudulent charges, mitigation expenses, cost of prevention) and the advantages and drawbacks of possible options for own approaches to more effectively prevent cybercrime and cooperation with the public sector. The consultation will be conducted in part through the European Cybercrime Centre Advisory Group on Financial Services, which unites a number of stakeholders from the financial services industry that assist Europol in improving the fight against cybercrimes affecting the financial services industry.

The consultations of **civil society** will notably focus on identifying the impact, including any long-term effects, on the lives of victims of non-cash payment fraud that e.g. led to a negative credit history or other negative impacts, in addition to other aspects of fundamental rights including data protection. On these issues, the Fundamental Rights Agency (FRA) should also be consulted.

Finally, consultation of **law enforcement and the judiciary** including Europol and Eurojust will serve to confirm the description and scale of the problem as the basis for action and help assess the possible positive and negative impacts of the policy options under consideration from an operational perspective. This will include the meetings that take place in the context of the EMPACT Policy Cycle priority on Non-Cash Payment Fraud, which brings together experts from the EU Member States and the EEA at Europol four times a year to discuss progress made, new modi operandi, and issues for law enforcement action. Furthermore, operational action days organised by Europol such as the Airline Fraud Action Day will serve to highlight further issues in transnational cooperation.

Will an Implementation plan be established?

☐ **Yes** ☒ **No**

D. Information on the Impact Assessment Process

The Commission Impact Assessment work should start in May 2016. The evaluation of the current situation will be integrated into the Impact Assessment Report, as a distinct part of the latter explaining the main findings of the evaluation and the position of the Commission on the evaluation results.

An Interservice Steering Group to help guide the overall process was set up in April 2016; this steering group will also cover the impact assessment stage. Participating Directorates-General should include as a starting point the Secretariat-General; the Legal Service; DG HOME; DG JUST; DG CNECT; DG MOVE; OLAF; DG GROW; DG DIGIT; DG FISMA; DG ECFIN; DG COMP; DG TAXUD; the Joint Research Centre (JRC) and the European External Action Service (EEAS).

As mentioned above, a study outsourced to an external contractor will help inform the Commission Impact Assessment exercise.

E. Preliminary Assessment of Expected Impacts

Likely economic impacts

Subject to further assessment, the likely economic impacts would include:

- On the negative side, for both the public and the private sector, the administrative and opportunity costs associated with implementing new legislation including trainings etc. For the private sector, further costs could arise e.g. from an increased investment in public-private cooperation.
- On the positive side, a more effective fight against non-cash payment fraud could potentially reduce the

costs incurred by the retail sector and the financial services industry which[33] currently bear the majority of the direct financial impacts, while consumers suffer both from the pass on of these costs through retail prices and increased banking charges related to their payment instruments including cards or their bank account as banks incorporate the costs of fraud in the fees they charge. Customers could benefit from lower retail prices as merchants are charged for fraud and to a lesser extent from lower fees if financial services providers pass on lower fraud costs through their fees. Furthermore, if the measures succeed in creating more trust in the digital single market, this could positively affect participation rates and therefore also the overall growth rate and take-up. Given that currently 12% of respondents to a recent Eurobarometer Survey stated that they avoid online banking and 15% avoided shopping online, both for security reasons, this could result in significant additional economic benefits, even when accounting for the likely positive effect of increased security afforded by the PSD2 and the NIS directive.

Likely social impacts

If a legislative instrument including strengthened victims' rights is pursued, this would have a positive effect on the economic and possibly also psychological situation of victims. Furthermore, effective repression of crimes that create harm to society, resulting in successful prosecution of those crimes, should entail a corresponding positive effect on society.

Likely environmental impacts

None

Likely impacts on simplification and/or administrative burden

The overall administrative burden for companies is low as criminal law rules are implemented and enforced by the State and there is no need to adapt internal policies or processes to such rules. A certain additional administrative burden could arise from reinforced public-private cooperation. This will need to be carefully assessed, also on the basis of quantitative data.

However, this would also result in a simplification as there currently is no legal certainty for financial institutions and payment service providers, as the rules differ in from Member State to Member State.

Likely impacts on SMEs

SMEs would most likely be involved only as victims of non-cash payment fraud. If they are the direct victim whose finances are affected, their position would be strengthened if the option of better protecting victims is retained. In the case of a small bank, a certain administrative burden could be associated with strengthened public-private cooperation. However, reporting on cyber incidents and card fraud is already required at present for regulatory purposes. As a result, the additional burden should be relatively limited for small-scale financial institutes.

Likely impacts on competitiveness and innovation

If the central objective of increasing trust in the digital single market is achieved, there might be an indirect positive impact from expanded use of online services in the internal market.

Likely impacts on public administrations

The public sector would incur administrative and opportunity costs associated with negotiating, transposing and implementing new legislation, including trainings etc. Furthermore, administrative burden and costs may be associated with requests to provide statistical data, with reinforced victims' rights or the provision of specific investigative tools. It can also not be excluded that a higher maximum level of sanctions will provoke more imprisonment sentences and, as a consequence, costs for detention. On the positive side, easier international cooperation between law enforcement agencies is to be expected, as they would share the same definition of criminal offences and – depending on the selected policy option – might benefit from specific measures to strengthen cooperation such as dedicated contact points. This could reduce the efforts required to conduct a cross-border investigation and could result in swifter and more successful prosecution of cases.

Likely impacts on third countries, international trade or investment

No significant impacts on any of the above are to be expected, except for a possible indirect positive impact stemming from a better functioning digital single market; common EU-wide definitions may simplify the cooperation with third countries related to the criminal phenomenon on a political and law enforcement level as the partner countries could rely on a more coherent response across the EU.

[33] Merchants are charged for almost all online payment fraud, which represents 66% of all fraud, which suggests banks in the first instance bear 33% of costs.