Council of the European Union

Brussels, 11 July 2023
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	10 July 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 363 final
Subject:	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

Delegations will find attached document COM(2023) 363 final.

Encl.: COM(2023) 363 final

EUROPEAN
COMMISSION

Brussels, 10.7.2023
COM(2023) 363 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

1. Introduction

Fraud and counterfeiting of non-cash means of payment such as credit or payment cards are a source of income for organised crime and enable other criminal activities such as terrorism, drug trafficking and trafficking in human beings. These crimes cause significant losses: the total value of fraudulent transactions using cards issued within the Single Euro Payments Area (SEPA) amounted to €1.87 billion in 2019.[1] The vast majority of fraudulent transactions are related to card-not-present (CNP) fraud: in 2019 80% of the value of card fraud resulted from CNP transactions, i.e. payments via the internet, mail or phone.[2] CNP fraud accounted for €1.50 billion in fraud losses in 2019, up by 4.3% on the previous year.[3]

There is a clear cross-border dimension: More than half of the total value of fraud in 2019 was related to cross-border transactions within SEPA. From a geographical perspective, domestic transactions accounted for 89% of the value of all card transactions in 2019, but only 35% of fraudulent transactions. Cross-border transactions within SEPA represented 9% of all card transactions in terms of value, but 51% of reported fraud.[4]

To fight these crimes effectively, Member States need to commonly define what acts should be considered fraud and counterfeiting of non-cash means of payment. They also need approximated levels of sanctions and the operational means to report offences and exchange information between authorities. Accordingly, on 17 April 2019, the European Parliament and the Council adopted Directive 2019/713 (the 'Directive') on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.[5] This report responds to the requirement under Article 21 of the Directive.

1.1. Objectives and scope of the Directive

The objectives of the Directive are to approximate the criminal law of the Member States[6] in the area of fraud and counterfeiting of non-cash means of payment and to improve cooperation between competent authorities. To this end, the Directive establishes minimum rules concerning the definition of criminal offences and sanctions. The scope of the Directive is wide, covering any "non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange," Art. 2(a)[7]. For example, a mobile payment application in conjunction with the authorisation procedure (e.g. PIN) would be covered by this definition. It includes also virtual currencies, Articles 2(d) and 6.

---

[1] European Central Bank, Seventh report on card fraud, available at https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG.

[6] From this point onwards and unless explicitly indicated differently, 'Member States' or 'all Member States' refer to the Member States bound by the Directive, i.e. all EU Member States except Denmark and Ireland, which did not take part in the Directive's adoption, in accordance with the Protocol on the position of Denmark annexed to the Treaty on the European Union and to the Treaty on the Functioning of the European Union (TFEU) and in accordance with Protocol 21 on the position of the United Kingdom and Ireland, respectively.

[7] All Articles mentioned refer to those of the Directive unless indicated otherwise.

The Directive defines specific criminal offences, namely:

- Fraudulent use of non-cash payment instruments (Article 3);
- Offences related to the fraudulent use of corporeal non-cash payment instruments (Article 4);
- Offences related to the fraudulent use of non-corporeal non-cash payment instruments (Article 5);
- Fraud related to information systems (Article 6);
- Illegal provision of tools used for committing the mentioned offences (Article 7).

In addition, the Directive **extends criminal liability** to incitement, aiding and abetting by natural and/or legal persons to commit and their attempt to commit the offences mentioned above (Article 8).

Minimum levels for the maximum **penalties** for offences referred to in the Directive are provided for in Article 9.

The subsequent Articles set up minimum conditions for the **liability of legal persons** (Article 10) and sanctions, which shall include criminal or non-criminal fines, and provide an exemplary list of other sanctions against them (Article 11).

The objective of Article 12 is to ensure that the offenders as set out in the Directive face prosecution in respect of the offences under Articles 3 to 8 of the Directive. A Member State's **jurisdiction** have to be established if a) the offence is committed in whole or in part on its territory, and/or b) the offender is one of its nationals. In other words, Article 12(1), point (a) of the Directive sets out the territoriality principle while point (b) leads to the principle of active nationality.

Article 13(1) of the Directive stipulates that **investigative tools** for investigating and prosecuting the offences referred to in Articles 3 to 8 should be effective, proportionate and available to the responsible persons, units and services. Information regarding the offences referred to in Articles 3 to 8 should reach the authorities investigating or prosecuting those offences without undue delay, according to Article 13(2) of the Directive.

Regarding exchange of information, Article 14 requires Member States to ensure that they have operational national **points of contact** available 24 hours a day and 7 days a week, so that they can reply to any urgent foreign request within 8 hours.

Furthermore, Article 15(1) of the Directive requires Member States to set up appropriate channels to **report the offences** referred to in Articles 3 to 8 to public authorities without undue delay. In particular financial institutions are invited to report suspected fraud to law enforcement and judicial authorities (Article 15(2)). Reporting is often the starting point of criminal investigations (Recital 27).

Finally, Articles 16 and 17 of the Directive deal with **assistance and support to victims** and **prevention** respectively.

1.2 Purpose and methodology of the report

Article 20 of the Directive requires Member States to bring into force the laws, regulations and administrative provisions necessary to comply with the Directive by 31 May 2021 and communicate them to the Commission.

This report responds to the requirement under Article 21 of the Directive for the Commission to report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive. The report – which is the first under Article 21 – provides an overview of the main transposition measures taken by Member States.

Member State transposition involved collecting information on the relevant legislation and administrative measures, analysing it, drafting new legislation or — in most cases — amending existing acts, seeing it through to adoption and finally reporting it to the Commission.

By the transposition date (31 May 2021), 9 Member States had notified the Commission that they had fully completed the Directive's transposition and communicated their transposition measures. In July 2021, the Commission opened infringement procedures for non-communication of national transposition measures against the remaining 16 Member States: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO and SI[8]. While 15 Member States have since notified their transposition measures, as of 30 April 2023, an infringement procedure for non-communication of national transposition measures against BG is still pending.[9]

The subsequent description and analysis in this report are based on the information on national transposition measures that Member States provided by 31 January 2023. Notifications received after that date have not been taken into account. All notified measures referring to national legislation were taken into account as well as court decisions and – where appropriate – common legal theory. Furthermore, during the course of the analysis, the Commission contacted Member States directly where appropriate for additional information or clarifications. All the information gathered was taken into consideration for the analysis.

Beyond the issues identified in this report, there may be further challenges in transposition and other provisions not reported to the Commission or future legislative and non-legislative developments. Therefore, this report does not prevent the Commission from further evaluating some provisions and from continuing to support Member States in the transposition and implementation of the Directive.

[8] Member States in this document are abbreviated according to: http://publications.europa.eu/code/en/en-5000600.htm.

[9] Information on the Commission's decisions on infringement procedures can be found at: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

2. Transposition measures

2.1 Legal definitions

Article 2 lays out the definitions of the main terms used in the Directive, namely: non-cash payment instrument; protected device, object or record; digital means of exchange; virtual currency; information system; computer data; legal person.

Member States have generally transposed the definitions by relying on laws pre-dating the Directive or adopted after its entry into force. In some instances, while there are no provisions specifically laying out definitions, the offences are transposed through general provisions of the criminal code that have a broader scope, e.g. provisions on theft. Therefore, non-communication of a verbatim transposition of the definition does not necessarily indicate non-completeness or non-conformity.

Furthermore, several of the definitions cross-reference definitions laid out in other directives.

a) Non-cash payment instruments

The assessment has revealed at least one one instance of incomplete transposition, as the definition set by the Council Framework Decision 2001/413/JHA had not been updated. Consequently, it refers only to corporeal payment instruments and does not cover 'protected device, object or record, or a combination thereof', as provided in the Directive's definition.

b) Protected device, object or record

Several Member States have not transposed this definition (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). This is not necessarily considered as an instance of non-compliance as, typically, the meaning is self-explanatory or can be derived from the wording of the definition of non-cash payment instrument. In some countries, the concept is explained in preparatory works.

c) Digital means of payment and virtual currency

These two definitions are central to Directive 2019/713, whose main objective was to address the fact that Framework Decision 2001/413/JHA no longer reflected the current realities and insufficiently addressed new challenges and technological developments such as virtual currencies and mobile payments which needed to be included to ensure a comprehensive response to the phenomenon and close unintended gaps in criminalisation.

The main issue encountered in transposition is the coverage of virtual currency, defined in Article 2(d) of the Directive. While electronic money is defined in all Member States, often as a result of the transposition of the E-money Directive[10], the definition and coverage of virtual money is not always straightforward.

[10] 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, OJ L 267, 10.10.2009

In HU, virtual currency is considered as property and electronic data, and can be subject to confiscation of property and seizure. Similarly, in PL, virtual currency is not defined in legislation and there is a certain level of uncertainty as to whether it would be covered by the different offences relevant to the transposition of the Directive, although some authors consider that virtual currency could fall under provisions of the Criminal Code regulating offences relating to information, data carrier or information data.

Many Member States have transposed these definitions through financial rules rather than in criminal laws (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). However, not in all these cases, there is a cross-reference to the relevant provisions in the national legislation setting the offences. Finally, in three Member States (IT, MT, RO), both definitions are transposed in the Criminal Code.

d) Information system

Article 2(e) defines 'information system' by cross-referring to point (a) of Article 2 of Directive 2013/40/EU. All Member States have transposed the definition in conformity with the Directive.

e) Computer data

Computer data is defined in Article 2(f) by cross-reference to point (b) of Article 2 of Directive 2013/40/EU. All Member States have transposed Article 2(f) in conformity with the Directive.

f) Legal person

Finally, Article 2(g) defines 'legal person'. Close to all Member States have transposed this term in their legislation. The only exception is SE, which does not define 'legal person'. The closest term used in the transposition is 'undertaking'. This term is neither defined in any legal text, nor in doctrine or case law.

2.2 Specific criminal offences

a) Fraudulent use of non-cash payment instruments

Article 3(a) of the Directive requires Member States to take the necessary measures to ensure that the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument, when committed intentionally, is punishable as a criminal offence.

25 Member States transposed Article 3(a) of the Directive. Out of the 25 countries, 14 transposed the Directive through a provision specifically on the fraudulent use of non-cash payment instruments (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). The remaining Member States referred to more general offences, such as fraud and computer counterfeiting, or fraud related to means of payments, not limited to non-cash payment instruments (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

HR law does not refer to the use of stolen or otherwise unlawfully appropriated payment instruments; the transposing provision in HU refers only to electronic non-cash payment instruments.

According to Article 3(b) of the Directive, Member States shall take the necessary measures to ensure that the fraudulent use of a counterfeit or falsified non-cash payment instrument, when committed intentionally, is punishable as a criminal offence.

Article 3(b) was generally transposed in a complete manner.

To transpose the Directive, 15 Member States refer to national provisions on non-cash payment instruments (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), while the national transposing legislation in ten Member States covers more general offences such as theft or fraud, or offences related to payment instruments, but not specifically non-cash instruments (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Offences related to the fraudulent use of corporeal non-cash payment instruments

Article 4 of the Directive requires Member States to take the necessary measures to ensure that the intentional acts listed within its sub-paragraphs are punishable as a criminal offence. The subparagraphs include the theft or other unlawful appropriation of a corporeal non-cash payment instrument (a); the fraudulent counterfeiting or falsification of a corporeal non-cash payment instrument (b); the possession of a stolen or otherwise unlawfully appropriated, or of a counterfeit or falsified corporeal non-cash payment instrument for fraudulent use (c); the procurement for oneself or another, including the receipt, appropriation, purchase, transfer, import, export, sale, transport or distribution of a stolen, counterfeit or falsified corporeal non-cash payment instrument for fraudulent use (d).

While Article 4 mostly appears to have been transposed in a more or less literal manner, in a few instances the national transposition raises questions when it comes to the specific acts of procurement for oneself or another of a stolen, counterfeit or falsified corporeal non-cash payment instrument for fraudulent use.

c) Offences related to the fraudulent use of non-corporeal non-cash payment instruments

Article 5 of the Directive criminalises conducts linked to the fraudulent use of non-corporeal non-cash payment instruments. The analysis found that this Article does not appear to have created challenges in transposition. In the majority of the cases, the national provision applies to both corporeal and non-corporeal non-cash payment instrument. About half of the Member States have transposed Article 5 of the Directive through a more general provisions (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), and more than half of them have transposed it through a provision relating specifically to the fraudulent use of non-cash payment instruments (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Fraud related to information systems

Article 6 of the Directive obliges Member States to ensure that performing or causing a transfer of money, monetary value or virtual currency, and thereby causing an unlawful loss of property for another person in order to make an unlawful gain for the perpetrator or a third party, is punishable as a criminal offence, when committed intentionally by, without right, hindering or interfering with the functioning of an information system (Art. 6(a)); or, without right, introducing, altering, deleting, transmitting or suppressing computer data (Art. 6(b)). All Member States have transposed Article 6.

e) Tools used for committing offences

Article 7 of the Directive requires Member States to take the necessary measures to ensure that producing, procurement for oneself or another, or making available a device or an instrument, computer data or any other means primarily designed or specifically adapted for the purpose of committing any of the offences referred to in Articles 4(a)-(b), 5(a)-(b) or 6, at least when committed with the intention that these means be used, is punishable as a criminal offence.

The vast majority of Member States have transposed Article 7 of the Directive (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Six countries have transposed Article 7 of the Directive through provisions, which cross-refer to broader provisions, either on general offences such as theft, or concerning financial instruments and means of payments (BG, FI, FR, LV, SE, SK). 17 countries have transposed it through a specific provision on tools used for committing the different offences of the Directive related to corporeal or non-corporeal non-cash payment instruments (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Five Member States appear to have faced challenges in transposition (BE, BG, HU, PL, PT).

2.3 General rules for the offences concerned

a) Incitement, aiding and abetting; attempt

Under Article 8(1) of the Directive, Member States need to ensure that inciting or aiding and abetting an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

All Member States have transposed this provision. The vast majority of the Member States have transposed the Directive through a pre-existing article on incitement, aiding and abetting in general (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). However, two Member States decided to enact a new provision, which applies only in the context of the Directive's offences (CY, MT).

Article 8(2) first sentence of the Directive requires Member States to ensure that an attempt to commit an offence contained in Article 3, Articles 4(a), (b) or (d), Articles 5(a) or (b), or Article 6 is punishable as a criminal offence. All Member States appear to have transposed this provision in a complete manner, except for BE, LU and SI.

Here again, the majority of Member States have transposed the Directive through a previously existing provision applying to attempt in general (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). The others have included it in a special transposing measure (CY, DE, FI, MT, RO).

Member States also need to ensure that at least the attempted fraudulent procurement of an unlawfully obtained, counterfeit or falsified non-corporeal non-cash payment instrument for oneself or another (Article 5(d)) is punishable as a criminal offence, Article 8(2) second sentence.

The assessment revealed that the criminalisation of the attempt may be subject to limitations not provided for in the directive in two Member States (HR, SI).

All remaining Member States transposed the relevant provisions of the Directive. They did so either through an article on attempt in general (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK), or through a special transposing measure (CY, DE, FI, MT, RO).

b) Penalties

Article 9 stipulates that the offences in Articles 3 to 8 be punishable by effective, proportionate and dissuasive criminal penalties, and provides the maximum term of imprisonment for the different offences.

While Member States have generally transposed Article 9 of the Directive, the assessment identified possible issues relating to the scope of the definition regarding Article 9(2) in HR, and 9(6) in BE, CZ, HR and HU.

The comparison of the sanctions set by Member States for the different offences is complicated because the offences are covered by both general and specific provisions. When they transposed the Directive through provisions on general offences, Member States have relied on several national provisions to criminalise one of the acts prohibited by the Directive. This leads to several maximum penalties applicable to this specific offence and implies that the actual maximum sanction would depend on each specific case, on the approach followed by the Courts and on national rules on concurrent sanctions. As an example, in PL, the rule is that one act can only constitute one offence. In case a conduct has features of two or more provisions of criminal law, the Court must choose one specific offence. On the contrary, in BG, in cases where the Special part of the Criminal Code provides for the imposition of two or more penalties concurrently for a certain crime, the court shall determine the extent of each penalty such that the sum complies with the general objectives of the penalty.

Furthermore, provisions may contain aggravating circumstances which may raise the ceiling and lead to increased sanctions. The maximum penalty therefore depends on the way the offence is committed. For instance, the general provision on misappropriation in HR carries a maximum penalty of five years' imprisonment. However, if the offender uses force, the maximum penalty is 10 years, and if the action resulted in substantial material gain, the offender faces up to 12 years of imprisonment. In DE, falsifying corporeal non-cash payment instruments leads to a maximum of five years of imprisonment. Yet, if the offender acted with a commercial purpose, the penalty will be of maximum 10 years.

The assessment also revealed that, in most cases, the thresholds provided for in the domestic legislation are more stringent than those set by the Directive. The difference can be significant: counterfeiting money is punishable by up to 15 years in BG and LU and up to 25 years in PL. Only two Member States provide for the same (or very close) maximum penalties as the ones of the Directive (AT, MT).

c) Liability of legal persons

The assessment showed that 16 Member States have transposed Article 10 of the Directive through an already existing general provision of their Criminal Code (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), while nine Member States have transposed it through a law specifically on liability of legal persons in the context of the Directive (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sanctions for legal persons

Article 11 of the Directive requires Member States to set effective, proportionate and dissuasive sanctions in the form of criminal or non-criminal fines also for legal persons. All Member States have laid out such sanctions.

Article 11 provides an option for the Member States to include various specific sanctions for legal persons, such as the exclusion from entitlement to public benefits or the judicial winding-up. Six Member States did not make use of the option in Article 11 of the Directive at all (AT, BG, EE, FI, NL, SE). The remaining 19 countries have either transposed the whole Article 11, or parts of it (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Jurisdiction

This Article, obliging Member States to establish jurisdiction for offences committed on their territory or by a national, is transposed in the general provisions of the national Criminal Code or Criminal Procedural Code in all Member States. Therefore, the territoriality principle and the principle of active nationality are of general application and not specific to the offences regulated by this Directive. Additionally, Article 12 was also transposed by CY in the national Law on Combatting of Fraud and Counterfeiting of Non-Cash Means of Payment Law, and by PT in the Cybercrime Law.

All Member States transposed Article 12(1) points (a) and (b).

Article 12(3) allows Member States to establish jurisdiction over an offence referred to in Articles 3 to 8 of the Directive committed outside their territory, where, inter alia, a) the offence is committed by someone who has his / her habitual residence in its territory; b) the offence is committed for the benefit of a legal person established in its territory; or c) the offence is committed against one of its nationals or a person who is a habitual resident in its territory. Fourteen Member States (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) have made use of the option laid down in Article 12(3)(a); 12 Member States (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) transposed Article 12(3)(b); and 16 Member States (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) have extended their jurisdiction in accordance with Article 12(3)(c). With regard to this point (c), in BG, DE, EE, HU, RO and SI, jurisdiction has been established over an offence committed outside its territory where the offence is committed (only) against one of its nationals – thus omitting habitual residents. AT provides for prosecution by the Austrian criminal justice system for offences committed abroad if the perpetrator and the victim are Austrians. CY, CZ, EL, FI, LV and MT have made use of all three optional provisions laid down in Article 12(3).

2.4 Operational issues

a) Effective investigations and cooperation

In all Member States, investigative tools for investigating and prosecuting the offences referred to in Articles 3 to 8 are not explicitly included in the legislation transposing the Directive, but rather in more general legislation, such as Codes of Criminal Procedure. Typically, the possibility to use an investigative tool in a certain case is related to the sanction for the offence in question; thus, as already hinted at in the Directive provision, the investigative tools used in countering organised crime or in other serious crime cases will also be available to investigate and prosecute the offences laid down in this Directive. The exceptionality of some investigative tools and the need of proportionality with the offence is most often included in the relevant legal provisions and/or in the Constitution.

Information regarding the offences referred to in Articles 3 to 8 should reach the authorities investigating or prosecuting those offences without undue delay, according to Article 13(2) of the Directive. In other words, law enforcement authorities and other competent authorities should have timely access to relevant information in order to investigate and prosecute the offences referred to in this Directive (Recital 22). The Code of Criminal Procedure often provides for various reporting systems so that criminal offences (within the meaning of Articles 3 to 8 of the Directive) can be reported efficiently and quickly. These reporting systems include: a duty to report of public bodies and authorities; a whistle-blowing system; a complaint procedure; an obligation of payment service providers to report serious operational or security incidents; and a right of private individuals to report incidents. Further, some more specific laws can ensure that reports of security incidents (including reports of serious criminal acts, such as unauthorised acquisition, forgery and alteration of a means of payment) are reported to the relevant authorities as quickly as possible. Such laws were reported by AT, CZ, LT, FI, MT and PT.

The condition that the submitted information should "reach the relevant authorities without undue delay" is most often not transposed explicitly.

b) Exchange of information

The exchange of information among national law enforcement authorities for the purposes of investigating and prosecuting crimes, including those referred to in Article 3 to 8 of the Directive, can be facilitated through operational points of contacts (Recital 26). Article 14(1) first sentence of the Directives ensures that Member States indeed establish those points of contact and that they are available 24/7. Further, the second sentence obliges Member States to have procedures in place to deal promptly with urgent requests for assistance and to provide a reply within eight hours, by at least indicating whether the request will be answered and the form of such an answer and the estimated time within which it will be sent.

The following Member States decided to make use of an existing operational point of contact for the purposes described in this Directive: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Table 1 provides an overview of the established points of contact. No points of contact were identified in BG, CZ, LU, SI, HR.

Table 1 Operational Points of Contact

MS	Point of Contact	MS	Point of Contact
AT	Federal Criminal Police Office	**EE**	Ministry of Justice
BE	Directorate for Operational Police Information	**FI**	National Bureau of Intelligence
BG	N/A	**FR**	Division for international relations of the Central Directorate of the judicial police

CY	Cyprus Police	**HR**	N/A
CZ	N/A	**HU**	International Criminal Cooperation Centre (NEBEK)
DE	16 State Criminal Police Offices and one Federal Criminal Police Office - Central Cybercrime Contact Points	**MT**	Malta Police Force
EL	Hellenic Police (International Police Cooperation Division)	**ES**	Emergency Coordination Cell
IT	International Operations Room of the Service for International Police Cooperation	**NL**	National Centre for International Legal Assistance (LIRC)
LT	2nd Division of the Force Management Board of the Police Department under the Ministry of the Interior of the Republic of Lithuania and the International Relations Board of the Lithuanian Criminal Police Bureau	**PL**	General Police Headquarters
LV	National Police	**PT**	Criminal Police
RO	Prosecution and Criminal Investigation Section of the General Prosecutor's Office	**SE**	Police Authority
SI	N/A	**SK**	Criminal Police Bureau of the Presidium of the Police Force of the Slovak Republic

Article 14(1) second sentence of the Directive has been practically implemented in a few Member States. Information on the procedures that apply to urgent requests could not be found in BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Reporting of crime

Member States are also obliged to make avaliable appropriate reporting channels. Such channels to report suspected fraud or, more generally, to report any possible criminal offences, can be laid down in legislative acts. Often, Member States have established the reporting of a crime as an obligation for certain categories of (natural and legal) persons (much in line with Article 15(2)), while victims and other 'bystanders' are given the possibility (but not the obligation) to report. These legal provisions are usually complemented by practical implementations.

In all Member States, written or oral reports can be made to the police and/or the judiciary. In addition, some Member States have provided additional reporting channels:

AT federal law provides for various reporting systems so that criminal offences within the meaning of Articles 3 to 8 of the Directive can be reported efficiently and quickly: 1) the duty to report of public bodies and authorities; 2) the whistle-blowing system of the Office of the Public Prosecutor for Economic Affairs and Corruption; 3) the whistle-blowing system of the Financial Market Authority; and 4) the obligation of payment service providers to report serious operational or security incidents. A specific reporting office for cybercrime has been established at the Federal Criminal Police Office. In addition, the Federal Ministry of the Interior is cooperating with the Federal Economic Chamber. As a result, various mailings and campaigns are taking place, motivating and encouraging the public to report relevant violations of the law.

In BE, the Ministry of Economy manages a single point of contact for victims of fraud, scam, deception and swindling. In addition, a whistleblowing channel has been legally established and made available by the Financial Services and Markets Authority for all complaints related to credit or investment products and services.

In CY, the Cyprus Police, together with the Central Bank of Cyprus and the national authority for the security of network and information systems, are formally designated through a legislative measure as the competent national authorities responsible for the establishment of appropriate channels of reporting and communication.

CZ criminal law obliges State authorities to report.

In DE, obliged entities are required without undue delay to report suspicious transactions. In addition, non-legislative measures have been adopted at Federal level, such as an institutionalised public-private partnership for the purpose of detecting, preventing, investigating or prosecuting offences referred to in Articles 3 to 8 of the Directive, and a platform for the exchange of information.

In EL, in addition to the general reporting channels, the Greek government has set up an online state service where citizens may directly submit complaints for criminal offences committed online. In addition, credit institutions and other providers of payment services must report to the Bank of Greece (which has competences concerning such complaints) any incidence of fraud immediately as they encounter it.

In ES, apart from general channels of offences reporting, the Bank of Spain provides reporting channel in collaboration with the National Cybersecurity Institute.

Italian legislation ensures timeliness in the communication to the public prosecutor by the judicial police of the news of an offence, acquired on their own initiative or following a complaint or a lawsuit. Information sharing is also encouraged through digital platforms.

LT has multiple reporting channels to report offences referred to in Articles 3 to 8 of the Directive, via an internet webpage (e-Police Portal), via the general emergency telephone number 112, in-person, by e-mail, by text message and through the e-Police mobile application, and other automatic means. Payment service providers, financial institutions and other obliged entities, the Bank of Lithuania and the Financial Crime Investigation Service are obliged to notify the competent law enforcement authorities of reasonable suspicions of criminal and/or other unlawful actions.

In LU, a website explaining how to report frauds is available. The Financial Sector Control Commission set guidelines to detect financial fraud but also requests that all establishments under its supervision to report as soon as possible any frauds and any incidents due to external computer attacks.

In RO, there is an obligation to report for public servants and persons holding managerial positions within public authorities, persons performing services of public interest and persons acting within control and supervision bodies.

In SI there is a duty to report a criminal offence for all state authorities and organisations with public authority.

The Perceval platform in FR, established by a legal act, allows victims to report on bank card fraud and counterfeiting. A similar platform exists for reporting on cybercriminality. Further, sanctions apply to any (natural or legal) person that does not prevent by his/her immediate action a crime, hence leading to a general obligation to report.

In HU, the obligation to report a criminal offence is only set for the members of the authority, public officers and statutory professional bodies. The Hungarian National Bank encourages on its website financial institutions, in the form of an opinion, to report suspected fraud.

In MT, the national point of contact encourages reporting, in particular by financial institutions, of suspected fraud and counterfeiting of non-cash means of payment.

Apart from the legally established whistleblowing reporting channel in PT, there is a "one-click" Cybercrime Reporting System available, where it is possible to follow a link that instantly opens an email directed to the competent authorities.

In SE, certain types of crime, such as credit card fraud, can also be reported via the Police Authority's e-service. Also, actors in banking and financing activities are obliged to report suspicious activities related to potential cases of money-laundering or terrorist financing, or property that otherwise derives from a criminal act to the Police Authority. In addition, an ongoing dialogue is kept between banking and finance operations and the Police Authority's National Fraud Center.

Legal provisions in SK set out a requirement (and procedures) of public authorities and other legal persons to forthwith report criminal offences to the law enforcement authorities. There are also reporting obligations relating to money laundering of obliged persons and specifically of banks.

Alternatively, non-legislative actions implementing Article 15 of the Directive have taken place in NL and PL. The Dutch police service lines and the website of the police provide an appropriate channel to report fraud which involves non-cash means of payment to the authorities. Further, the Dutch government has committed to encouraging financial institutions and other legal persons to report any suspicion of fraud. The effort is apparent by, for example, the existence of a front office for financial fraud which is installed in all police units in the Netherlands. Also, four major banks and ICS cards have signed a covenant with the police to jointly combat (banking) fraud and phishing. In PL, reports of crimes are accepted 24/7 by all police units. Additionally, due to the nature of crimes committed with the use of computer technologies, it is possible to contact them directly with a specialised organisational unit of the Police Headquarters. Further, in order to ensure the fastest possible cooperation with the banking sector, a cooperation channel has been established between the Bureau for Combating Cybercrime of the Police Headquarters and the Banking Security Centre of the Polish Bank Association.

Article 15(2) of the Directive has not been transposed in BG, EE, HR.

2.5 Support to victims and prevention

a) Assistance and support to victims

Asistance and support to natural and legal persons whose personal data has been misused is ensured by Article 16(1) of the Directive. Measures should include: a) the offering of specific information and advice on protection against the negative consequences of such crime, and b) the provision of a list of dedicated institutions covering different aspects of identity-related crime and victim support.

In the same vein, legal persons that are victims of the offences referred to in Articles 3 to 8 of this Directive should have access to information about a) the procedures for making complaints, b) the right to receive information about the case, c) the available procedures for making complaints if the competent authority does not respect the victim's rights in the course of criminal proceedings, and d) the contact details for communications about their case (Article 16(3) of the Directive).

The Code of Criminal Procedure of most Member States contains regulations on victims and their rights, including some specific provisions on the victims' rights to information and assistance during proceedings, the right to counselling and the right to complain. A specific Act transposing the Directive often complements what has already been set out in the Code of Criminal Procedure. Legal persons are typically treated in separate legal provisions within the Code of Criminal Procedure, or elsewhere. Additionally, various information campaigns, leaflets, dedicated websites, circulars, etc are available to assist and support victims of the offences referred to in Articles 3 to 8 of the Directive. This is the case in AT, BE (with regard to Article 16(1)), CY, CZ, DE, IT, LT , LU (with regard to Article 16(1)), LV (with regard to Article 16(3)), RO, SI (with regard to Article 16(3)), EE, FI (with regard to Article 16(1)), FR (with regard to Article 16(1)), HR, HU, NL, PL (with regard to Article 16(3)), PT, SE and SK. Article 16(1) and/or Article 16(3) of the Directive have nowhere been literally or almost literally transposed, with the exception of MT.

The list of accredited counselling facilities that provide assistance to victims, as referred to under point b) of Article 16(1) of the Directive, is normally available online, hence implemented in practice.

b) Prevention

Article 17 on prevention requires Member States to take appropriate action, e.g. information and awareness-raising campaigns, research and education programmes. This section is based on an assessment of the information notified by the Member States to the Commission as well as an open source Internet research to explore the existence of prevention measures. As described in Table 2 below, when prevention actions have been identified, these relate principally to cybercrime and online fraud. However, in some countries, information on prevention of fraud is also provided, typically by the Police.

Table 2 Prevention Actions

MS	Actions
AT	The Federal Police regularly provides information on its website and in social networks about ways to protect oneself against fraud. Cooperation with stakeholders such as the Chamber of Commerce is supported and implemented within the framework of e-commerce projects.
BE	Different websites with advice/awareness raising materials, such as those run by the Centre for Cybersecurity Belgium (CCB). Some cooperation with stakeholders could be identified through internet search e.g. the organisation representing the financial sector have cooperated with the Brussels public prosecutor office (parquet) to develop awareness raising materials
BG	A campaign to fight "financial mules" in Bulgaria started in 2021 run by the Association of Banks and carried out jointly with the General Directorate "Fight against Organised Crime" and the prosecutor's office. The General Directorate has also launched a campaign on phishing
CY	The Cybercrime Subdivision of the Police provides on its website information and advice on issues such as digital fraud as well as information on upcoming events, e.g. awareness-raising campaigns. One example is the information campaign on information security carried out by the Police, the Central Banks, the Banks Association and the Digital Security Authority.
DE	Federal Police (BKA) provides on its website an overview of the measures aimed at institutionalized public-private partnership for the purpose of detecting, preventing, investigating or prosecuting the offences covered by the Directive, e.g. the partnership between the Federal Criminal Police Office (BKA), the Federal Office for Information Security (BSI) and the "German Competence Centre against Cyber Crime e.V." (G4C), an association of financial institutions and companies from the IT security sector. BKA also launched the Cybercrime Conference C³, a platform for exchange between authorities, business, science and politics. G4C also produces information brochures and training. Finally, the BKA also participates in prevention measures in the area of cybercrime at Länder level and, at the national level, the BKA is also networked with other police and non-police authorities and organisations (stakeholders) and is stepping up cooperation, especially on trend topics.
FR	The Ministry of Interior is publishing information on cyber prevention. Platforms available to report cybercrime also includes prevention messages as well as the National Police Information and Communication Service (SICoP). Other examples include guidance issued by the Bank of France or the guide on prevention against fraud published by the National Task Force on the fight against fraud, which groups different administration and enforcement authorities.
EL	The Cyber Crime Division and the Police Headquarters are very active in informing the public, raising awareness and reducing the risk of becoming a victim of fraud, with TV campaigns, educational speeches and online information.
ES	The Spanish National Cybersecurity Institute and the Tax Agency provide in their website relevant information to prevent phishing, ransomware etc. in business environments.
HR	The Ministry of Interior provides online information about internet frauds and runs a Youtube channel dedicated to "Fraud and Computer Security", containing videos about cyberscams
IT	The Treasury Department, which has the task of preventing fraud on means of payment, is already promoting a series of initiatives at local level, in collaboration with local administrations and the university system, organising seminars and workshops addressed to the categories involved in currency counterfeiting, including citizens
LT	Information on prevention can be found on the website of the Communications Regulation Authority in relation to online fraud and the website of the Police on the most common types of cyber fraud. In

	addition, one of the objectives of the National Strategy on Cybercrime is to strengthen the prevention and control of cybercrime, in particular by developing effective cooperation between law enforcement authorities and other stakeholders.
LV	The Financial and Capital Market Commission has developed various internet tools to provide information and guidance on financial security and fraud issues. In addition, various campaigns have been organised in cooperation with the State Police and the Consumer Rights Protection Centre.
NL	Measures are in place, such as the 'Fraudehelpdesk' (fraud helpline) an organisation subsidised by the Dutch Government. Where fraudulent actions can be reported, The Fraudehelpdesk is a part of the SAFECIN stichting (Foundation for Tackling Financial and Economic Crime in the Netherlands (SAFECIN)) a foundation with governmental involvement
SE	An ongoing dialogue is kept between banking and finance operations and the Police Authority's National Fraud Centre, NBC. In addition, NBC collaborates, also for crime prevention purposes, with e.g. actors in e-commerce. The importance of reporting fraud to the police is emphasised in these contacts.

In ten Member States (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK), no information on appropriate prevention actions and practical implementation was found, although in MT and RO, the legislation reflects this obligation, closely following the Directive's wording.

3. Conclusion and next steps

The Directive has led to substantive progress in criminalising fraud and counterfeiting of non-cash means of payment on a comparable level across the Member States, which facilitates the cross-border cooperation of law enforcement authorities investigating this type of offences. Member States have amended criminal codes and other relevant legislation, streamlined procedures, and set up or improved cooperation schemes. The Commission acknowledges the major efforts by the Member States to transpose the Directive.

However, there is still scope for the Directive to reach its full potential if Member States were to fully implement all of its provisions. The analysis so far suggests that some of the main improvements to be achieved by the Member States include Article 2(d), which provides the definition of virtual currency; Article 7 on offences related to the tools used for committing the offences, and Article 8(2) on attempt; Article 9(6) on penalties for natural persons in case the offence is committed in the framework of a criminal organisation; Article 14 on exchange of information; and Article 16 on assistance and support to victims.

The Commission will continue to provide support to the Member States in their implementation of the Directive. In particular, a dedicated call for proposals will be published in 2023.

The Commission is committed to ensuring that the transposition is finalised across the EU and that the provisions are correctly implemented. This includes monitoring that national measures comply with the corresponding provisions in the Directive. Where necessary, the Commission will make use of its enforcement powers under the Treaties through infringement procedures.