Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

DIRECTIVE (EU) 2019/713 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[(1)],

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) Fraud and counterfeiting of non-cash means of payment are threats to security, as they represent a source of income for organised crime and are therefore enablers for other criminal activities such as terrorism, drug trafficking and trafficking in human beings.

(2) Fraud and counterfeiting of non-cash means of payment also represent obstacles to the digital single market, as they erode consumers' trust and cause direct economic loss.

(3) Council Framework Decision 2001/413/JHA[(3)] needs to be updated and complemented in order to include further provisions on offences in particular with regard to computer-related fraud, and on penalties, prevention, assistance to victims and cross-border cooperation.

(4) Significant gaps and differences in Member States' laws in the areas of fraud and of counterfeiting of non-cash means of payment can obstruct the prevention, detection and sanctioning of those types of crime and other serious and organised crimes related to and enabled by them, and make police and judicial cooperation more complicated and therefore less effective, with negative consequences for security.

(5) Fraud and counterfeiting of non-cash means of payment have a significant cross-border dimension, accentuated by an increasing digital component, which underlines the need for further action to approximate criminal legislation in the areas of fraud and of counterfeiting of non-cash means of payment.

(6) Recent years have brought not only an exponential increase in the digital economy, but also a proliferation of innovation in many areas, including payment technologies. New

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

payment technologies involve the use of new types of payment instruments, which, while creating new opportunities for consumers and businesses, also increase opportunities for fraud. Consequently, the legal framework must remain relevant and up-to-date against the background of those technological developments, on the basis of a technology-neutral approach.

(7) Fraud is not only used to fund criminal groups, but also limits the development of the digital single market and makes citizens more reluctant to make online purchases.

(8) Common definitions in the areas of fraud and of counterfeiting of non-cash means of payment are important to ensure a consistent approach in Member States' application of this Directive and to facilitate information exchange and cooperation between competent authorities. The definitions should cover new types of non-cash payment instruments which allow for transfers of electronic money and virtual currencies. The definition of non-cash payment instruments should acknowledge that a non-cash payment instrument may consist of different elements acting together, for example a mobile payment application and a corresponding authorisation (e.g. a password). Where this Directive uses the concept of a non-cash payment instrument, it should be understood that the instrument puts the holder or user of the instrument in a position to actually enable a transfer of money or monetary value or to initiate a payment order. For example, unlawfully obtaining a mobile payment application without the necessary authorisation should not be considered as an unlawful obtainment of a non-cash payment instrument as it does not actually enable the user to transfer money or monetary value.

(9) This Directive should apply to non-cash payment instruments only insofar as the instrument's payment function is concerned.

(10) This Directive should cover virtual currencies only insofar as they can be commonly used for making payments. The Member States should be encouraged to ensure in their national law that future currencies of a virtual nature issued by their central banks or other public authorities will enjoy the same level of protection against fraudulent offences as non-cash means of payment in general. Digital wallets that allow the transfer of virtual currencies should be covered by this Directive to the same extent as non-cash payment instruments. The definition of the term ‘digital means of exchange’ should acknowledge that digital wallets for transferring virtual currencies may provide, but do not necessarily provide, the features of a payment instrument and should not extend the definition of a payment instrument.

(11) Sending fake invoices to obtain payment credentials should be considered as an attempt at unlawful appropriation within the scope of this Directive.

(12) By using criminal law to give legal protection primarily to payment instruments that make use of special forms of protection against imitation or abuse, the intention is to encourage operators to provide such special forms of protection to payment instruments issued by them.

(13) Effective and efficient criminal law measures are essential to protect non-cash means of payment against fraud and counterfeiting. In particular, a common criminal law

approach is needed as regards the constituent elements of criminal conduct that contribute to or prepare the way for the actual fraudulent use of a non-cash means of payment. Conduct such as the collection and possession of payment instruments with the intention to commit fraud, through, for instance, phishing, skimming or directing or redirecting payment service users to imitation websites, and their distribution, for example by selling credit card information on the internet, should thus be made a criminal offence in its own right without requiring the actual fraudulent use of a non-cash means of payment. Such criminal conduct should therefore cover circumstances where possession, procurement or distribution does not necessarily lead to fraudulent use of such payment instruments. However, where this Directive criminalises possession or holding, it should not criminalise mere omission. This Directive should not sanction the legitimate use of a payment instrument, including and in relation to the provision of innovative payment services, such as services commonly developed by fintech companies.

(14) With regard to the criminal offences referred to in this Directive, the concept of intent applies to all elements constituting those criminal offences in accordance with national law. It is possible for the intentional nature of an act, as well as any knowledge or purpose required as an element of an offence, to be inferred from objective, factual circumstances. Criminal offences which do not require intent should not be covered by this Directive.

(15) This Directive refers to classical forms of conduct, like fraud, forgery, theft and unlawful appropriation that had already been shaped by national law before the era of digitalisation. The extended scope of this Directive with regard to non-corporeal payment instruments therefore requires the definition of equivalent forms of conduct in the digital sphere, complementing and reinforcing Directive 2013/40/EU of the European Parliament and of the Council[(4)]. The unlawful obtainment of a non-corporeal non-cash payment instrument should be a criminal offence, at least when it involves the commission of one of the offences referred to in Articles 3 to 6 of Directive 2013/40/EU or the misappropriation of a non-corporeal non-cash payment instrument. ‘Misappropriation’ should be understood to mean the action of a person entrusted with a non-corporeal non-cash payment instrument, to knowingly use the instrument without the right to do so, to his own benefit or to the benefit of another. The procurement for fraudulent use of such an unlawfully obtained instrument should be punishable without it being necessary to establish all the factual elements of the unlawful obtainment and without requiring a prior or simultaneous conviction for the predicate offence which led to the unlawful obtainment.

(16) This Directive also refers to tools which can be used in order to commit the offences referred to in it. Given the need to avoid criminalisation where such tools are produced and placed on the market for legitimate purposes and, though they could be used to commit criminal offences, are therefore not in themselves a threat, criminalisation should be limited to those tools which are primarily designed or specifically adapted for the purpose of committing the offences referred to in this Directive.

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

(17) The sanctions and penalties for fraud and counterfeiting of non-cash means of payment should be effective, proportionate and dissuasive throughout the Union. This Directive is without prejudice to the individualisation and application of penalties and execution of sentences in accordance with the circumstances of the case and the general rules of national criminal law.

(18) As this Directive provides for minimum rules, Member States are free to adopt or maintain more stringent criminal law rules with regard to fraud and counterfeiting of non-cash means of payment, including a broader definition of offences.

(19) It is appropriate to provide for more severe penalties where a crime is committed in the framework of a criminal organisation, as defined in Council Framework Decision 2008/841/JHA[(5)]. Member States should not be obliged to provide for specific aggravating circumstances where national law provides for separate criminal offences and this may lead to more severe sanctions. When an offence referred to in this Directive has been committed in conjunction with another offence referred to in this Directive by the same person, and one of those offences de facto constitutes a necessary element of the other, a Member State may, in accordance with general principles of national law, provide that such conduct is regarded as an aggravating circumstance to the main offence.

(20) Jurisdictional rules should ensure that the offences referred to in this Directive are prosecuted effectively. In general, offences are best dealt with by the criminal justice system of the country in which they occur. Each Member State should therefore establish jurisdiction over offences committed on its territory and over offences committed by its nationals. Member States may also establish jurisdiction over offences that cause damage in their territory. They are strongly encouraged to do so.

(21) Recalling the obligations under Council Framework Decision 2009/948/JHA[(6)] and Council Decision 2002/187/JHA[(7)], competent authorities are encouraged in cases of conflicts of jurisdiction to use the possibility of conducting direct consultations with the assistance of the European Union Agency for Criminal Justice Cooperation (Eurojust).

(22) Given the need for special tools to effectively investigate fraud and counterfeiting of non-cash means of payment, and their relevance to effective international cooperation between national authorities, investigative tools that are typically used for cases involving organised crime or other serious crime should be available to competent authorities in all Member States, if and to the extent that the use of those tools is appropriate and commensurate with the nature and gravity of the offences as defined in national law. In addition, 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. Member States are encouraged to allocate adequate human and financial resources to the competent authorities in order to properly investigate and prosecute the offences referred to in this Directive.

(23) National authorities investigating or prosecuting offences referred to in this Directive should be empowered to cooperate with other national authorities within the same Member State and their counterparts in other Member States.

(24) In many cases, criminal activities are behind incidents that should be notified to the relevant national competent authorities under Directive (EU) 2016/1148 of the European Parliament and of the Council[8]. Such incidents may be suspected to be of a criminal nature even if there is insufficient evidence of a criminal offence at that stage. In such a context, relevant operators of essential services and digital service providers should be encouraged to share the reports required under Directive (EU) 2016/1148 with law enforcement authorities so as to form an effective and comprehensive response and to facilitate attribution and accountability by the perpetrators for their actions. In particular, promoting a safe, secure and more resilient environment requires systematic reporting of incidents of a suspected serious criminal nature to law enforcement authorities. Moreover, when relevant, computer security incident response teams designated under Directive (EU) 2016/1148 should be involved in law enforcement investigations with a view to providing information, as considered appropriate at national level, and also to providing specialist expertise on information systems.

(25) Major security incidents as referred to in Directive (EU) 2015/2366 of the European Parliament and of the Council[9] may be of criminal origin. Where relevant, payment service providers should be encouraged to share with law enforcement authorities the reports they are required to submit to the competent authority in their home Member State under Directive (EU) 2015/2366.

(26) A number of instruments and mechanisms exist at Union level to enable the exchange of information among national law enforcement authorities for the purposes of investigating and prosecuting crimes. To facilitate and speed up cooperation among national law enforcement authorities and make sure that those instruments and mechanisms are used to the fullest extent, this Directive should strengthen the importance of the operational points of contact introduced by Framework Decision 2001/413/JHA. It should be possible for Member States to decide to make use of the existing networks of operational points of contact, such as the one set up in Directive 2013/40/EU. The points of contact should provide effective assistance, for example by facilitating the exchange of relevant information and the provision of technical advice or legal information. To ensure the network runs smoothly, each point of contact should be able to communicate quickly with the point of contact in another Member State. Given the significant trans-border dimension of crimes covered by this Directive and in particular the volatile nature of electronic evidence, Member States should be able to deal promptly with urgent requests from the network and provide feedback within eight hours. In very urgent and serious cases, Member States should inform the European Union Agency for Law Enforcement Cooperation (Europol).

(27) Reporting crime to public authorities without undue delay is of great importance in combating fraud and counterfeiting of non-cash means of payment, as it is often the starting point of criminal investigations. Measures should be taken to encourage reporting by natural and legal persons, in particular financial institutions, to law enforcement and judicial authorities. Those measures can be based on various types of action, including legislative acts containing obligations to report suspected fraud, or non-legislative actions, such as setting up or supporting organisations or mechanisms