DOI 10.5817/MUJLT2020-2-5

MISUSE OF CONTACTLESS PAYMENT CARDS WITH RADIO-FREQUENCY IDENTIFICATION

by

LIBOR KLIMEK*

Counterfeiting of means of payment is one of European crimes. The Treaty on the Functioning of the European Union lists counterfeiting of means of payment as one of the areas of particularly serious crime with a cross-border dimension. At the European Union level a brand-new legislative instrument harmonising counterfeiting of means of payment has been adopted – the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means of payment. Moreover, it facilitates the prevention of such offences, and the provision of assistance to and support for victims. The Directive is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

The contribution deals with criminalisation of the misuse of contactless payment cards with Radio-Frequency Identification (RFID) technology. It is divided into three sections. The first section focuses on definition of Radio--Frequency Identification and payment cards with Radio-Frequency Identification. The second section focuses in detail on a new European Union approach to combat counterfeiting of means of payment addressed to its Member States – i.e. the Directive (EU) 2019/713 on combating fraud and counterfeiting of non--cash means of payment. The last third section is focused on non-legislative prevention possibilities.

* libor.klimek@umb.sk, Associate Professor at the Department of Criminal Law, director of the Criminology and Criminalistics Research Centre at the Faculty of Law, Matej Bel University in Banská Bystrica, Slovak Republic. Visiting Professor at the Faculty of Law, Leipzig University, Germany. Advisor of the Constitutional Court of the Slovak Republic.

KEY WORDS

Criminal Offences, Criminalisation, Directive (EU) 2019/713 on Combating Fraud and Counterfeiting of Non-Cash Means of Payment, Payment Cards with Radio--Frequency Identification, Prevention, Radio-Frequency Identification (RFID), Sanctions

1. INTRODUCTION

Payment cards have become very popular among people. Moreover, contactless payments by payments cards, introduced in 2007, have become popular as well. These days one in three card payments is contactless. Contactless payments are payments made by waving or tapping such card over a reader, which accepts the payment (if there are no barriers, for example, if payment limit of card is exceeded or if the validity of card has expired).

Payment cards have a chip inside them that recognises radio waves, if a card holder wishes to pay contactless. It is based on *Radio-Frequency Identification technology* – known as *RFID*. On the one hand, such a payment method is very useful method in case of small payments, for example, payments up to 20 EUR. On the other hand, there are many ways to misuse cards. In October 2016 the *Daily Mail*[1] revealed that criminals can swipe money off RFID cards – i.e. payment cards using contactless payments – as people are walking down the street, sitting in a restaurant or browsing in shops.

2. RADIO-FREQUENCY IDENTIFICATION AND PAYMENT CARDS WITH RFID

RFID uses wireless communication to establish the identity of a physical object. Automatic identification is the primary functionality provided by RFID technology, enabling recognition of tagged objects. Consequently, RFID tagged objects or persons can be easily recognised.[2] RFID is a system that transmits the identity of an object wirelessly, using radio waves. RFID tag is attached to an object and contains information about it.

---

[1] Could you fall prey to a contactless conman? How thieves can take money from your card as you're walking down the street. [online] Available from: https://www.dailymail.co.uk/news/article-3849368/Could-fall-prey-contactless-conman-thieves-money-card-walking-street.html [Accessed 18 October 2016].

[2] Ahson, S. A., Ilyas, M. (2008) *RFID Handbook: Applications, Technology, Security, and Privacy*. Boca Raton: CRC Press, p. 644.

Since the recent past RFID is understood as advanced automatic identification technology.[3] The basic technologies for RFID have been around for long time. Its root can be traced back to an espionage device designed in 1954 by *Léon Theremin* (*Lev Sergeyevich Termen*, Russian: *Лев Сергеевич Термéн*) of the Soviet Union, which retransmitted incident radio waves modulated with audio information.[4]

There are several versions of RFID that operate at different radio frequencies. Three primary frequency bands are used for RFID:

- *Low-Frequency* – 125/134 Khz – most commonly used for attendance and access control;
- *High-Frequency* – 13,56 MHz – used where medium data rate and read ranges up to about 1,5 meters are acceptable; it is used in case of contactless payment cards; and
- *Ultra-High-Frequency* – 850 to 950 MHz – offers the longest read ranges of up to approximately 3 meters and high reading speeds.

These days we use payment cards (also known as, for example, bank cards, ATM cards, client cards or cash cards). The most common payments cards are *debit cards*[5] and *credit cards*[6], provided by, for example, *Visa*, *Mastercard* or *Maestro*. They offer also contactless payments, since they have a small microchip inside that is capable of emitting radio waves. The antenna and chip are both built into the plastic. Such contactless cards operate at only a short range – 1–5 centimetres (or more) and work on RFID technology.

---

[3] Nof, S. Y. (2009) *Springer Handbook of Automation*. Berlin – Heidelberg: Springer, p. 865; Han, Z., Xu, Y., Wang, R. (2014) The Summarize of Medium Access Control Protocol in RFID. In: Xue Wang, Li Cui, Zhongwen Guo (eds.). *Advanced Technologies in Ad Hoc and Sensor Networks: Proceedings of the 7th China Conference on Wireless Sensor Networks*. Heidelberg – New York – Dordrecht – London, Springer, p. 336.

[4] Qiao, Y., Chen, S., Li, T. (2012) *RFID as an Infrastructure*. New York – Heidelberg – Dordrecht – London: Springer, p. 1.

[5] A *debit card* is a payment card made of plastic that contains chips. It is commonly used instead of cash in order to make payment(s). The money is transferred directly from the cardholder's bank account to merchant's bank account.

[6] A *credit card* is a payment card made of plastic that contains chips. It is commonly used instead of cash in order to make payment(s). It enables the cardholder to pay a merchant based on the cardholder's promise to the card issuer to pay for the amounts (plus the other agreed financial charges). The card issuer creates a revolving account and grants a line of credit to the cardholder. It means that the money is not transferred directly from the cardholder's bank account to merchant's bank account, but the cardholder "borrows" money for payment(s) in order to pay a merchant.

To pay with a contactless payment card, for example, in a supermarket or in a restaurant, the customer holds their card near to the reader, i.e. RFID reader. Consequently, the reader can communicate with the card's microchip. Further, the reader sends to the card the details regarding transaction, the card sends back the payment details and then the payment processor processes the contactless payment. Such understanding of using contactless payments can be illustrated in the more expanded series of events:[7]

- the RFID reader establishes a connection with the card;
- the RFID reader sends the card an encryption key;
- the card decrypts the encryption key, which allows all future communication to be encrypted using that key;
- the card reader sends the card the proposed transaction;
- the card creates a transaction document, including payment details;
- the card "signs" the transaction document using its private key;
- the card sends the transaction document to the card reader; and
- the card reader sends a receipt to the card.

The very first advantage of RFID technology is that it is convenient method of payment. An RFID reader sends needed information to the card. Card holder does not need to know all details of payment(s). This allows faster processing of payments. In general, unlike *bar code readers*[8] or *QR code readers*[9] that can only scan a single code at once, RFID readers are able to communicate with multiple tags at once.

RFID chips are small enough that they could be placed in payment card. Indeed, the card holder on the first touch does not know that the card has extra chip inside. These days the payment cards include such a chip quite commonly. Such a chip is placed commonly on the corner of the card, what is indicated by special symbol on the card.

---

[7] How Do RFID Contactless Payments Work? [online] Available from: https://www.cards witcher.co.uk/2019/03/rfid-contactless-payments/ [Accessed 8 November 2019].

[8] A *bar code* is a method of representing data in a visual form, which is machine-readable. It was invented in the United States of America in 1951. Today, bar codes are used in many contexts, especially when shopping. They are pre-printed on most items in shops. This speed up processing at check-outs.

[9] A *QR code* – abbreviated from *Quick Response code* – is a label, which is machine-readable, that contains information about the item to which it is attached. It was first designed in 1994 in Japan. The QR system became popular due to its fast readability and greater storage capacity compared to bar code.

RFID technology allows real-time usage of payments. If the card is close RFID reader, the payment does not require more than a few seconds. It is faster than using payment with PIN (personal identification number) and much faster than payment by cash. The reason is that it is not needed to calculate the value of banknotes and coins before payment.

As seen, the advantages of using RFID technology are persuasive. On the other hand, it is important to note that RFID technology has disadvantages as well.

It is easy to misuse RFID chip in payment card. Anyone with a fake RFID scanner, even homemade scanner, can "send" signal. That means that anyone with a scanner can walk down the street and "scan" cards of people without realising it. Of course, PIN technology can reduce such danger, but it is not always working. Many cards using RFID technology have set limits for automatic approvals of payments, for example, up to 20 EUR.

Any wireless or contactless technology has the chance to be hacked, including RFID. If it is for payment purposes, it could create an identity theft issue. RFID readers could record the data of the card without permission of the card holder. If information is "stolen", RFID chips are very easy to clone and to be counterfeited.

RFID identity theft, sometimes called *RFID skimming*[10], occurred. Like most technologies and networks, RFID systems are also vulnerable to physical and electronic attacks, namely reverse engineering, power analysis, eavesdropping, sniffing, denial of service, cloning, spoofing and viruses. As this technology matures and finds numerous applications, hackers will continue to seek novel methods to access private information, infiltrate secure networks, and take the system down for their own gains.[11]

It should be noted that, fraud on contactless payment cards remains low. Available data are from the United Kingdom, for example. According to *UK Finance*[12] fraud using the contactless technology on payment cards and

[10] See, for example: Walker, M. (2019) *CEH Certified Ethical Hacker All-in-One Exam Guide*. 4th ed. New York: McGraw Hill Professional, p. 430; Fernándes-Caramés, T. M., Fraga--Lamas, P., Suárez-Albera, M., Castedo, L. (2017) A Methodology for Evaluating Security in Commercial. In: Paulo Crepaldi, Tales Pimenta (eds.). *Radio Frequency Identification*. Rijeka: InTech, p. 39.

[11] What Is RFID Skimming? [online] Available from: https://www.tripwire.com/state-of-security/featured/what-rfid-skimming/ [Accessed 8 November 2019].

[12] *UK Finance* is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, it seeks to enhance competitiveness, support customers and facilitate innovation. The Economic Crime team within *UK Finance* is responsible for leading the industry's collective fight against economic crime in the United Kingdom, including fraud, anti-money laundering, sanctions, anti-bribery, corruption and cybercrime.

devices remains low, with 19,5 million GBP of losses during 2018, compared to spending of 69 billion GBP over the same period. This is equivalent to 2,7p in every 100 GBP spent using contactless technology, the same level recorded in 2016 and 2017. Fraud using the contactless technology on payment cards and devices represents just 2,9 % of overall card fraud losses.[13]

3. EUROPEAN UNION APPROACH TO COMBAT COUNTERFEITING OF MEANS OF PAYMENT

3.1. COUNTERFEITING OF MEANS OF PAYMENT AS EUROPEAN CRIME

The general policy objective of the European Union is to ensure a high level of security through measures to prevent and combat crime.[14] At the European Union level some of criminal offences are considered as European crimes or so-called Euro crimes[15] (in literature there can be observed also the terms Euro-crimes[16] and Eurocrimes[17]).

Specific offences are recognised as offences which are within the legislative competence of the European Union. The *Treaty on the Functioning of the European Union* lists *counterfeiting of means of payment* as one of the areas of particularly serious crime with a cross--border dimension. It stipulates that

> *"*[t]*he European Parliament and the Council* [of the European Union] *may, by means of* directives *adopted in accordance with the ordinary*

[13] UK Finance. (2019) *Fraud the Facts 2019: The definitive overview of payment industry fraud*, p. 23. [online] Available from: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf [Accessed 8 November 2019].

[14] Article 67(3) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[15] It should be noted that the *Treaty on the Functioning of the European Union* does not use the wording *Euro crimes*. It is used by the *European Commission* – see: European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final, p. 5. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf. [Accessed 8 November 2019].

[16] See: Cools, M. et al. (2009) *Readings on Criminal Justice, Criminal Law & Policing*. Antwerpen – Apeldoorn: Maklu, p. 100; Miettinen, S. (2013) Criminal Law and Policy in the European Union. Abingdon – New York: Routledge, p. 145; Body-Gendrot, S. et al. (2014) *The Routledge Handbook of European Criminology*. Abingdon – New York: Routledge, p. 65; Chalmers, D., Davies, G., Monti, G. (2014) *European Union Law*. 3rd ed. Cambridge: Cambridge University Press, p. 657.

[17] See: Klip, A. (2012) *European Criminal Law: An Integrative Approach*. 2nd ed. Cambridge – Antwerp – Portland: Intersentia, p. 211.

> *legislative procedure, establish minimum rules concerning the* definition of criminal offences and sanctions *in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption,* counterfeiting of means of payment, *computer crime and organised crime* […]"[18] (emphasis added).

It should be noted that the *United Nations* and the *Council of Europe* have introduced conventions harmonising almost all of European crimes, generally even before the EU. Thus, taking into account legislation of the European Union and the conventions of the *United Nations* and the *Council of Europe*, one could observe "double criminalising" or even "triple criminalising" of some offences.

Within the European Union have been adopted legislative instruments regulating European crimes. There is no need to introduce their in-depth analysis, since this article is focused on *counterfeiting of means of payment*. The text below analyses the leading legislative instrument harmonising counterfeiting of means of payment – the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

3.2. DEFINITION OF CRIMINAL OFFENCES AND SANCTIONS: DIRECTIVE (EU) 2019/713

At the European Union level the leading legislative instrument harmonising counterfeiting of means of payment is the *Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment*[19] (hereinafter referred to as "Directive (EU) 2019/713"). This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means

[18] Article 83(1) of the Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[19] 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. *Official Journal of the European Union* (L 123/18) 10 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN [Accessed 8 November 2019].

of payment. Moreover, it facilitates the prevention of such offences, and the provision of assistance to and support for victims.[20]

The Directive (EU) 2019/713 repealed its predecessor – the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment.[21] It no longer reflected today's realities and insufficiently addresses new challenges and technological developments such as virtual currencies and mobile payments.[22] It was adopted in 2001, however, in 2013, fraud using cards issued in the *Single European Payment Area (SEPA)* reached 1,44 billion EUR, representing growth of 8 % on the previous year. An evaluation of the Framework Decision 2001/413/JHA identified three main problems that were driving the current situation concerning non-cash payment fraud in the European Union. First, some crimes could not be effectively investigated and prosecuted. Second, some crimes could not be effectively investigated and prosecuted due to operational obstacles. Third, criminals took advantage of gaps in prevention to commit fraud.[23] The *European Commission* introduced a proposal for a new legislation[24] addressed to the Member States of the European Union. It introduced three specific objectives that addressed the problems identified. First, to ensure that a clear, robust and technology neutral policy/legal framework is in place. Second, to eliminate operational obstacles that hamper investigation and prosecution and. Third, to enhance prevention.

---

[20] Article 1 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[21] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment. *Official Journal of the European Communities* (L 149/1) 2 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001F0413 [Accessed 8 November 2019].

[22] See: Funta, R. (2019) *Úvod do počítačového práva*. Brno, MSD, p. 67 *et seq.*; Ivor, J., Polák, P., Záhora, J. (2017) *Trestné právo hmotné II: Osobitná časť*. Bratislava: Wolters Kluwer, p. 212.

[23] For details see: European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019]; European Commission. (2017) *Impact assessment accompanying the Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Commission staff working document*, SWD(2017) 298 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/10102/2017/EN/SWD-2017-298-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

[24] European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

As seen, the Directive (EU) 2019/713 is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

The Directive (EU) 2019/713 contains own legal definitions. For the purpose of the Directive, non-cash payment instrument shall mean a 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.[25]

3.3. CRIMINAL OFFENCES

The Directive (EU) 2019/713 obliges the Member States of the European Union to introduce specific provisions into their criminal law or to modify existing provisions in this field. It establishes as criminal offences a number of acts committed intentionally, namely:

- fraudulent use of non-cash payment instruments;
- offences related to the fraudulent use of corporeal non-cash payment instruments;
- offences related to the fraudulent use of non-corporeal non-cash payment instruments; and
- fraud related to information systems.

As regards the misuse of contactless payment cards, relevant is the first group of above-mentioned offences, i.e. *fraudulent use of non-cash payment instruments*. The Directive (EU) 2019/713 stipulates that the Member States of the European Union shall ensure that, when committed *intentionally*, the following conduct is punishable as a criminal offence:

> *"the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument"*.[26]

---

[25] Article 2(a) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[26] Article 3 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. In addition, the act of inciting or aiding or abetting a person to mentioned offence may also lead to criminal liability.

In fact, the perpetrator of the offence does not use (misuse) the contactless card by his hand(s), since (s)he does not holds it. However, using fake RFID reader, (s)he sends the card an encryption key, subsequently the card decrypts the encryption key, which allows all future communication to be encrypted using that key, the card reader sends the card the proposed transaction, the card "signs" the transaction. On the one hand, the regular using of contactless payments operate at only a short range – 1-5 centimetres (or more). On the other hand, fake RFID reader can operate at longer distance, for example, a few meters.

As regards liability, the Directive (EU) 2019/713 defines the concept of criminal liability of natural persons as well as legal persons. Indeed, the Directive takes into account also corporate criminal liability.[27] On the other hand, the question which begs consideration is whether legal persons are interested in such a criminal offence.

It should be noted that criminal liability of legal persons for offences is an issue which has been coming and going on the political agenda of the European Union.[28] Another question which begs consideration in this context is whether liability of legal persons should be governed by civil or criminal controls. In the European Union the criminal law approach has evolved. Besides harmonisation of elements of crimes (European crimes) and sanctions for naturals, European Union law has repeatedly confirmed the liability of legal persons.[29] It became a common approach of legal framework regulating European crimes, including counterfeiting of means of payment.

---

[27] Article 10 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[28] Vermeulen, G., De Bondt, W., Ryckman, Ch. (2012) *Liability of Legal Persons for Offences in the EU*. Antwerpen – Apeldoorn – Portland: Maklu, p. 9; Maďar, M. (2016) Trestná zodpovednosť právnických osôb – historické aspekty. In: Dominika Cevárová (ed.). *Interpolis '16. Zborník vedeckých prác z XIII. medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov konanej dňa 10. novembra 2016 v Banskej Bystrici*. Banská Bystrica: Belianum, pp. 452–461.

[29] See, for example: Article 16 of the Directive (EU) 2017/541 on combating terrorism; Article 6 of the Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims; Article 13 of the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Article 7 of the Framework Decision 2004/757/JHA laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking; Article 6 of the Framework Decision 2003/568/JHA on combating corruption in the private sector; Article 11 of the Directive 2013/40/EU on attacks against information systems; Article 6 of the Framework Decision 2008/841/JHA on the fight against organised crime.

3.4. SANCTIONS FOR OFFENCES

The Directive (EU) 2019/713 defines serious environmental offences which should be made punishable under criminal law (see above). It obliges explicitly the States to provide for criminal sanctions in their criminal laws (see below).

The Directive stipulates, as regards sanctions for natural persons, that the Member States of the European Union shall ensure that the above--mentioned offences are punishable by *effective, proportionate and dissuasive criminal penalties*.[30] On the one hand, the Directive requires the Member States of the European Union to take *effective, proportionate and dissuasive sanctions*. On the other hand, it does not define this approach. According to the *European Commission*, *effectiveness* requires that the sanction is suitable to achieve the desired goal, i.e. observance of the rules; *proportionality* requires that the sanction must be commensurate with the gravity of the conduct and its effects and must not exceed what is necessary to achieve the aim; *dissuasiveness* requires that the sanctions constitute an adequate deterrent for potential future perpetrators.[31]

The Member States shall ensure that the some offences are punishable by a maximum term of imprisonment of at least one year, some at least two years and some at least three years.[32] In addition to that, the offences shall be punishable by a maximum term of imprisonment of at least five years if they are committed within the framework of a criminal organisation as defined in the Framework Decision 2008/841/JHA on the fight against organised crime[33] (irrespective of the penalty provided for in that Decision).

---

[30] Article 9(1) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non--cash means of payment.

[31] European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law.* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final, p. 9. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf [Accessed 8 November 2019].

[32] For details, see: Article 9(2)(3)(4)(5) of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[33] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime. *Official Journal of the European Union* (L 300/42) 11 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0841 [Accessed 8 November 2019]. The objective of the Framework Decision is to harmonise Member States' definitions of crimes related to a criminal organisation and to lay down corresponding penalties for these offences. See: Calderoni, F. (2010) *Organized Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organized Crime*. Heidelberg – Dordrecht – London – New York, Springer.

The Directive (EU) 2019/713 stipulates, as regards sanctions for legal persons, that the Member States of the European Union shall ensure that a legal person is subject to – again – *effective, proportionate and dissuasive sanctions*, which shall include criminal or non-criminal fines.[34]

4. NON-LEGISLATIVE PREVENTION

The prevention against misuse of payment cards with RFID chip is very simple. One could say that using of cash is the best protection. However, how about people constantly using payment cards, including contactless RFID payments.

RFID technology does not work through metal. One could pack their card in aluminium foil, but it is not comfortable. There is a possibility to use RFID-blocking products, for example, RFID card protector made of aluminium. It is small aluminium foil, where you can put your payment card. You can remove your card before payment and put it in the foil after payment. The price of such a foil is surprising – you can buy it just a few cents. For example, a pack of 10 aluminium foils costs about 1–5 EUR. On the other hand, there is opinion that RFID-blocking products are practically worthless. According to *Digital Trends*[35] a card transmits a one--time transaction code that is encrypted. It does not give name or billing address of its holder and crucially it does not include the three-digit code on the back of the card that is needed for online transactions. The information that can be skimmed is simply not enough to enable the thief to commit another crime. As regards RFID-blocking products,

> *"No, they're a waste of money,"*

Roger Grimes, data-driven defense evangelist at *KnowBe4*[36], told the *Digital Trends.*

> *"You shouldn't spend one cent. There has still to this day not been a report of a single real-world crime that an RFID blocking product would have stopped."*

[34] For details, see: Article 11 of the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment.

[35] RFID-blocking products are practically worthless. Here's why. [online] Available from: https://www.digitaltrends.com/cool-tech/are-rfid-blocking-products-worth-your-money-we-asked-an-expert/ [Accessed 8 November 2019].

[36] *KnowBe4* provides *Security Awareness Training* to help manage the IT security problems of social engineering, spear phishing and ransomware attacks. See: https://www.knowbe4.com

In personal banking, using two bank accounts is recommended – primary bank account and secondary bank account. While the primary bank account should be account for incomes, the secondary bank account should be used for outgoings – in case of credit cards all costs are paid via revolving account. It is good choice to send needed amount of money to secondary bank account and use payment card(s) issued to secondary bank account – not only for card payments by RFID and PIN, but also for all transactions – withdrawing money from an ATM (automated teller machine), online payments, mobile payments (for example, by *Masterpass*[37]), etc. If the card is misused (not only misuse for purposes of contactless payments), only limited amount of money will be lost.

5. CONCLUSION

Since the recent past RFID technology is understood as advanced automatic identification technology. As regards usage of this technology in banking, the very first advantage of this technology is convenience of payment. On the other hand, it is easy to misuse RFID chip in payment card. Anyone with a fake RFID scanner, even homemade scanner, can "send" signal. That means that anyone with a scanner can walk down the street and "scan" cards of people without realising it. Moreover, if information is "stolen", RFID chips are very easy to clone and to be counterfeited.

Specific offences are recognised as offences which are within the legislative competence of the European Union. The *Treaty on the Functioning of the European Union* lists *counterfeiting of means of payment* as one of the areas of particularly serious crime with a cross--border dimension. At the European Union level the leading legislative instrument harmonising counterfeiting of means of payment is the Directive (EU) 2019/713. This Directive establishes *minimum rules* concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means of payment. The Directive (EU) 2019/713 is addressed to the Member States of the European Union. They shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 31st May 2021.

[37] A *Masterpass* is a digital wallet offered by *Mastercard* to provide the consumers with a faster checkout process by storing the payment and shipping information at a secured location. See: https://www.masterpass.com

The Directive (EU) 2019/713 stipulates that the Member States of the European Union shall ensure that, when committed *intentionally*, the fraudulent use of a stolen or otherwise unlawfully appropriated or obtained non-cash payment instrument is punishable as a criminal offence.

As regards prevention against misuse of payment cards with RFID chip, it is very simple. RFID technology does not work through metal. One could pack their card in aluminium foil, but it is not comfortable. There is a possibility to use RFID-blocking products, for example, RFID card protector made of aluminium. It is small aluminium foil, where you can put your payment card. In personal banking, using two bank accounts is recommended. While the primary bank account should be account for incomes, the secondary bank account should be used for outgoings.

LIST OF REFERENCES

[1] Ahson, S. A., Ilyas, M. (2008) *RFID Handbook: Applications, Technology, Security, and Privacy*. Boca Raton: CRC Press.

[2] Could you fall prey to a contactless conman? How thieves can take money from your card as you're walking down the street. [online] Available from: https://www.dailymail.co.uk/news/article-3849368/Could-fall-prey-contactless-conman-thieves-money-card-walking-street.html [Accessed 18 October 2016].

[3] Council Framework Decision 2001/413/JHA of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment. *Official Journal of the European Communities* (L 149/1) 2 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001F0413 [Accessed 8 November 2019].

[4] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime. *Official Journal of the European Union* (L 300/42) 11 November. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008F0841 [Accessed 8 November 2019].

[5] 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. *Official Journal of the European Union* (L 123/18) 10 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN [Accessed 8 November 2019].

[6] European Commission. (2011) *Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 573 final. Available from: https://db.eurocrim.org/db/en/doc/1626.pdf [Accessed 8 November 2019].

[7] European Commission. (2017) *Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA*, COM(2017) 489 final. Available from: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-489-F1-EN-MAIN-PART-1.PDF [Accessed 8 November 2019].

[8] Fernándes-Caramés, T. M., Fraga-Lamas, P., Suárez-Albera, M., Castedo, L. (2017). A Methodology for Evaluating Security in Commercial. In: Paulo Crepaldi, Tales Pimenta (eds.). *Radio Frequency Identification*. Rijeka: InTech.

[9] Funta, R. (2019) *Úvod do počítačového práva*. Brno, MSD.

[10] Han, Z., Xu, Y., Wang, R. (2014) The Summarize of Medium Access Control Protocol in RFID. In: Xue Wang, Li Cui, Zhongwen Guo (eds.). *Advanced Technologies in Ad Hoc and Sensor Networks: Proceedings of the 7th China Conference on Wireless Sensor Networks*. Heidelberg – New York – Dordrecht – London, Springer.

[11] How Do RFID Contactless Payments Work? [online] Available from: https://www.cardswitcher.co.uk/2019/03/rfid-contactless-payments/ [Accessed 8 November 2019].

[12] Ivor, J., Polák, P., Záhora, J. (2017) *Trestné právo hmotné II: Osobitná časť*. Bratislava: Wolters Kluwer.

[13] Maďar, M. (2016) Trestná zodpovednosť právnických osôb – historické aspekty. In: Dominika Cevárová (ed.). *Interpolis '16. Zborník vedeckých prác z XIII. Medzinárodnej vedeckej konferencie doktorandov a mladých vedeckých pracovníkov konanej dňa 10. novembra 2016 v Banskej Bystrici*. Banská Bystrica: Belianum.

[14] Nof, S. Y. (2009) *Springer Handbook of Automation*. Berlin – Heidelberg: Springer.

[15] Qiao, Y., Chen, S., Li, T. (2012) *RFID as an Infrastructure*. New York – Heidelberg – Dordrecht – London: Springer.

[16] RFID-blocking products are practically worthless. Here's why. [online] Available from: https://www.digitaltrends.com/cool-tech/are-rfid-blocking-products-worth-your-money-we-asked-an-expert/ [Accessed 8 November 2019].

[17] Treaty on the Functioning of the European Union as amended by the Treaty of Lisbon. 26 October 2012 (C 326/47). Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:EN:PDF [Accessed 8 November 2019].

[18] UK Finance. (2019) *Fraud the Facts 2019: The definitive overview of payment industry fraud*. [online] Available from: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf [Accessed 8 November 2019].

[19] Vermeulen, G., De Bondt, W., Ryckman, Ch. (2012) *Liability of Legal Persons for Offences in the EU*. Antwerpen – Apeldoorn – Portland: Maklu.

[20] Walker, M. (2019) *CEH Certified Ethical Hacker All-in-One Exam Guide*. 4th ed. New York: McGraw Hill Professional.

[21] What Is RFID – Radio Frequency Identification? [online] Available from: https://www.iitms.co.in/rfid-based-attendance-system/what-is-rfid/ [Accessed 8 November 2019].

[22] What Is RFID Skimming? [online] Available from: https://www.tripwire.com/state-of-security/featured/what-rfid-skimming/ [Accessed 8 November 2019].