

Impact assessment of European policies for combating payment card fraud on the Stakeholders

Magdalena Atanasova^{1*}

¹Sofia University “St. Kliment Ohridski”, Sofia, Bulgaria

Abstract. The security of non-cash payment instruments is a key factor for the economic stability of the European Union. Crime with electronic payment instruments and related illegal activities affect the Digital Single Market and the financial interests of the European Union. Organized crime groups generate € 1.44 billion a year in the Community from payment card fraud, with illegal proceeds reinvested in illegal activity and not recovered. The current scientific article aims to assess an ex-post impact of European policies for combating payment card fraud and counterfeiting on the stakeholders, in particular payment process participants. The goal is to establish the policy efficiency by analyzing the cost and benefits of the specific policy for the participants. A methodology has been developed, based on a multidisciplinary approach. The following scientific methods are used: case study; research and review of legal and other documents; content analysis of strategic and annual reports and assessments; analysis of qualitative indicators and secondary analysis of empirical data. The results of the survey show that the cost of crime prevention and control measures is high, but responsibility for costs is shared between the public and private sectors, and consumers. Strengthening cooperation between stakeholders will lead to higher policy benefits and lower costs.

1 A problem statement

The penetration of information and communication technologies in all sectors of the contemporary world, incl. the banking sector, becomes an integral part of people's lives. The security of non-cash payment instruments (payment cards – debit and credit, credit transfers, direct debits, electronic money) is a key factor for the economic stability of the European Union. The existence of secure, efficient, competitive and innovative electronic payments is an important condition for consumers, retailers and the banking sector to reap the benefits of the Digital Single Market [1].

The topic of bank card crimes has become increasingly relevant over the last ten years. Payment card fraud and related illegal activities affecting the financial interests of the European Union represent significant losses for both the Union and society as a whole. They are low-risk and high-profit criminal activity. Payment card fraud is perpetrated by organized

* Corresponding author: atanasova.magi@yahoo.com

crime groups, which generate around € 1.44 billion a year in the Single Euro Payments Area (SEPA – covers all countries of the European Union, Iceland, Liechtenstein, Norway, Switzerland and Monaco). Illicit proceeds are reinvested in illegal activities and are not recovered [2]. This analysis focuses on bank card fraud, which is part of the crime with electronic payment instruments. For the purposes of the study, it is divided into two groups: "card-present" fraud at ATM and POS terminal (CP) and "card-not-present" fraud on the Internet, fax, telephone and mail (CNP).

2 Data and Methodology of the survey

This scientific article aims to assess an ex-post impact of European policies for combating payment card fraud and counterfeiting on the stakeholders, in particular payment process participants. The goal is to establish the policy efficiency by analyzing the cost and benefits of the specific policy for the participants. Trends over the last ten years have been followed, looking at strategic and legal documents since 2000, as Europe has been taking active policy-making action in this area. The secondary analysis of empirical data focuses from 2014 to 2018, discussing the data from the Sixth report on card fraud of the ECB.

The following sub-objectives (tasks) are set as a prerequisite for achieving the objective:

- to carry out a study on the use of payment cards, the value of payment transactions and fraud in CP and CNP, defining fraud as a share of the total value of transactions;
- to consider the level of security for CP and CNP inside and outside the European Union with cards issued in SEPA;
- to subsequently assess the impact of payment card fraud on participants in the payment process (the private sector represented by International Card Organizations, banking institutions, online and retail merchants, airlines, hotels, etc., on the one hand, and consumers, on the other hand) and in society as a whole;
- to determine the costs of payment card fraud – economic and non-economic costs, direct and indirect costs;
- to evaluate the effects and benefits of the policies for the participants in the payment process;
- to monitor the impact of the environment through the factors – external and internal;
- to compare the indicators and to evaluate the cost-benefit ratio of European policies for combating payment card fraud;
- to make forecasts for future risks and threats, and the corresponding preventive measures in the field of payment card fraud.

A methodology has been developed to achieve the objective and the relevant sub-objectives on the basis of which a multidisciplinary approach is applied. The following scientific methods are used: case study; research and review of legal and other documents; content analysis of strategic and annual reports and assessments; analysis of qualitative indicators and secondary analysis of empirical data.

Public policies are formed and implemented through various tools. As part of the multidisciplinary approach, separate categories of indicators have been developed and introduced: strategic, legal and other official documents; institutional and non-institutional stakeholders; technological and technical; operational and criminal; educational and tools for partnership and cooperation. The main subjects in the specific public policy are representatives of the three public sectors – public, private and civil. These are: business, European institutions and bodies (law enforcement agencies and judicial authorities, the European Central Bank, etc.), Member States, and the civil sector (NGOs, media, consumers, etc.).

Monitoring and evaluation provide accountability, i.e., information on the extent to which the policy achieves its objectives, how rationally public resources are used, what the public impacts are. They enable stakeholders to provide and receive information that is crucial for detecting abuses and protecting their interests [3]. According to the economic approach, policies that are a form of legitimate government interference in the natural order outlined by the market and competition are justified only if the benefits they create outweigh the cost of implementing them. Assessment of policy efficiency aims to prove that the benefit exceeds the cost of its creation. Achieving public goals – economic, political and social – benefits the community to which they apply, or all groups in it. Public policies are justified when they create public benefit, and it materializes in concrete products, results and impacts [4].

3 Results of the research

Payment cards are the most common electronic payment instrument for small payments, the use of which is increasing every year, both globally and in the European Union. According to the European Central Bank, the total value of card transactions issued in SEPA amounts to € 4.84 trillion in 2018, of which € 1.80 billion are fraudulent. Card fraud increased by 13% in value compared to 2017, while the value of all card transactions increased by 6.5%. Therefore, the value of card fraud is growing faster than the value of all card transactions, leading to an increase in fraud as a share of the total value of transactions from 0.002% points, from 0.035% in 2017 to 0.037% in 2018. But its level for 2018 remains below the five-year peak registered in 2015 (0.042%) (Fig.1) [5].

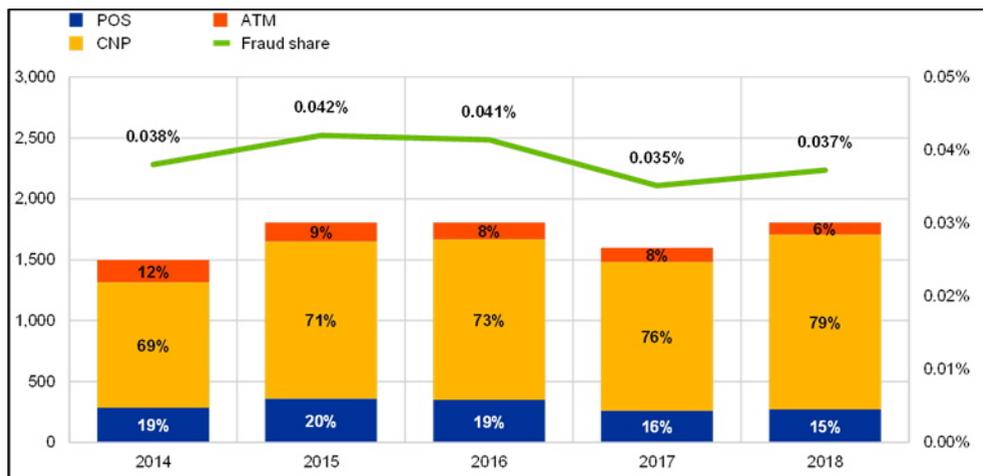


Fig. 1. Evolution of the total value of card fraud using cards issued within SEPA (left scale: total value of fraud (EUR mln.); right scale: value of fraud as a share of value of transactions (%))
 Source: European Central Bank, Sixth report on card fraud (2020)

During the reported years, CNP fraud increased as a share of the total value of card fraud, representing 79% in 2018, while the share of card fraud in ATMs and POS terminals decreased to 6% and 15% respectively in 2018 (Fig. 1). In addition, in 2018, the total value of CNP fraud increased by 17.7% compared to the previous year, reaching € 1.43 billion. This share has been growing steadily for the 10 years since 2008 and is in line with the ever-increasing importance of online card payments. The increase in CNP fraud by 39.31% over the five-year period, i.e., from 2014 to 2018, is the main driver of a 21% increase in total fraud during this period. The largest share of CNP fraud takes place across borders within SEPA (Fig. 2). However, cross-border transactions with cards issued in SEPA and acquired

worldwide accounted for a bigger share of fraudulent transactions (64%) in 2018 than domestic transactions within SEPA (36%) (Fig. 3). In general, countries with large card markets and widespread use of cards for online purchases have higher levels of fraud [5].

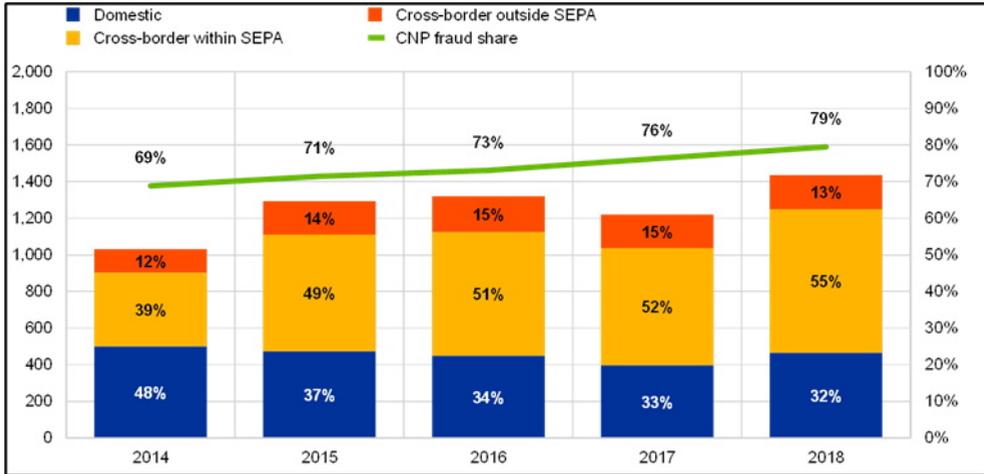


Fig. 2. Evolution of the value of CNP fraud and its share of the total value of card fraud (left scale: total value of CNP fraud (EUR mln.); right scale: value of CNP fraud as share of value of card fraud (%))

Source: European Central Bank, Sixth report on card fraud (2020)

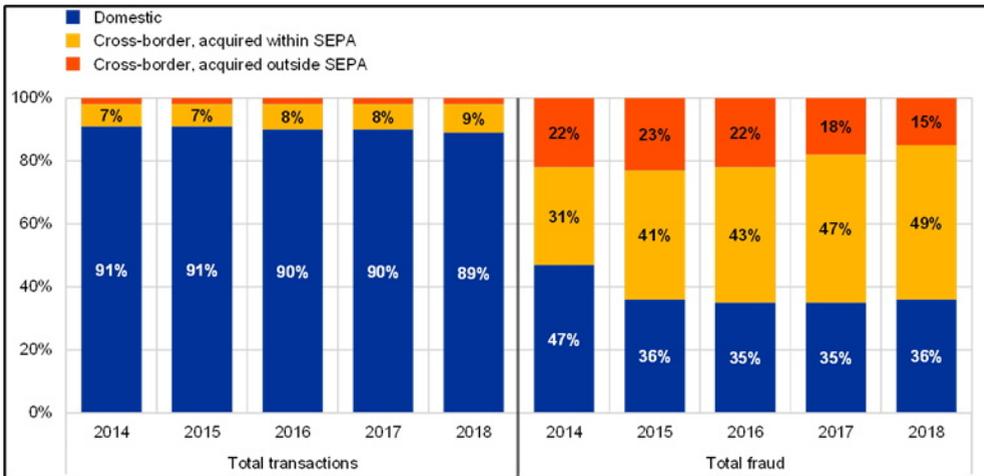


Fig.3. Evolution of the value of domestic and cross-border transactions and fraud (value of fraud or transactions by geographical breakdown as percentage of total (%))

Source: European Central Bank, Sixth report on card fraud (2020)

The process of formulating, implementing, monitoring, and evaluating European policies for combating payment card fraud is of particular importance for payment cards as an electronic payment instrument and the benefits of policies for stakeholders, incl. cardholders. The creation of the Single Euro Payments Area in 2005 at the initiative of the European Payments Council is a step in this direction. Adoption of the EMV standard (Europay, MasterCard® and Visa®) in the Member States with integrated chip card payment technology and introduction of a PIN code when making transactions is indicative of increasing the security of bank cards and reducing fraud on ATMs and POS terminals in the Community during the study period. The high level of protection of CNP directs criminals to

the weaknesses of the system in countries outside the European Union, where EMV technology is not fully implemented. These are countries in Asia (33.55%), North and South America (0.26%) [6], which in turn leads to significant losses for the Union. Increasing security measures for card-present payments is shifting the attention of offenders to card-not-present fraud. The data from the European Central Bank show that payment transactions made via the Internet, fax, telephone, and mail are subject to higher levels of fraud than traditional payment methods, most of which are made outside SEPA. Criminals target online retailers that have not adopted the 3-D Secure protocol standard [7], which is not mandatory in the Community and is not a global solution.

Therefore, due to the cross-border nature of payment card fraud and the high proportion of European card fraud outside the European Union, it is necessary to apply common international standards and security rules, and to take joint action between countries at the global level to prevent crime.

The negative impact of payment card fraud on society also has a negative effect on the economy, which hinders the development of the Digital Single Market in the European Union. The cost of fraud and counterfeiting of non-monetary means of payment can be economic or non-economic. The amount of financial losses from online payment card fraud exceeds the loss from "card-present" crimes. This causes huge damage, not only to the International Card Organizations Visa and MasterCard, payment card issuers, but also to airlines, hotels, online merchants, and retailers. Globally, airlines are among the hardest hit by CNP fraud, with losses of about \$ 1 billion a year as a result of buying plane tickets. According to VISA Europe, criminals commit fraud with airlines every three minutes, buying around 800 plane tickets every day in Europe through fraudulent transactions [8]. Payment card fraud provides revenue for organized crime and facilitates other criminal activities such as terrorism, drug and human trafficking, illegal immigration [9]. At the same time, the 2014 Verizon report notes that 2013 can be remembered as "a year of retail breakthroughs". However, the overall assessment shows that this is a year of transition from geopolitical attacks to large-scale attacks against card payment systems [10].

The real impact of payment card fraud is significant as a result of the costs associated with the crime. As fraud increases, there is an increase in retailers' spending from \$ 2.23 in 2015 to \$ 2.40 in 2016. This means that they pay an average of \$ 2.40 for a dollar of losses caused by crime with electronic payment instruments based on chargeback costs, fees, and exchange of goods [11]. In addition, traders incur costs in terms of insurance services, fraud management and crime prevention. Consumers also incur fraud prevention measures. In the event of irregular payment transactions, losses may be incurred by banks, merchants and / or cardholders according to the responsibility of the parties [12].

In Europe, Value Partners estimated the value of card fraud committed by criminals against consumers at more than € 3 billion in 2012 and forecast an increase, despite reductions as part of total costs. Globally, payment card fraud is expected to increase despite the introduction of fraud prevention technologies such as two-step authentication for access to online transactions, EMV technology and the adoption of 3-D Secure by e-merchants [13]. Covid-19 led to a 5% increase in card payments in 2020 and an increase in contactless payments, the shift to online shopping and the avoidance of cash for hygiene reasons [14]. The pandemic stimulated the issuance of new cards and at the same time the growth of fraud with them. Losses will reach \$ 28.65 billion worldwide in 2019. Nilson Report data show that the United States alone is responsible for more than a third of the total global loss, making it the most prone to card fraud. Global fraud losses are expected to increase to \$ 35.67 billion in five years and \$ 40.63 billion in 10 years, according to The Nilson Report [16].

Given the significant resources spent on the private and public sectors, this type of crime has both economic and non-economic costs. In case of payment card fraud and breach in the systems of banking institutions, their reputation is reduced, and the volume of payment

transactions is reduced. The feeling of insufficient security and protection leads to distrust and fear in their clients. It follows that, payment card fraud has a negative impact on banks, the security and convenience of cardholders.

A study by the European Commission shows that in 2013, 35% of European citizens have concerns about the security of remote payments, which is a reluctance to use online services [17]. Michael Levi and Jim Handley (2002) add the psychological and emotional effect of payment card fraud to consumers. The pilot interviews conducted by the researchers show that the victims are more likely to be surprised as an affected party in the crime than to perceive it only as a financial loss. A British crime study reported the following emotional reactions to deception (in descending order): anger, shock, fear, insomnia and crying [18].

According to Burelli et al. financial fraud has a negative impact on the economy, with the monetary value of fraud being a small part of the total cost to society [13]. The authors divide the costs of financial fraud into direct and indirect costs. Direct costs include: costs to the victim, regardless of the possible recovery of losses; costs for financial institutions and merchants as a result of a disputed payment; costs of anti-fraud measures, incl. prevention, investigation and prosecution; possible costs of resources used to prevent, investigate and prosecute criminals; increased cost for customer loans due to higher risk and related investigation costs; possible costs for less frequent use of the account due to a subsequent fraud event.

Indirect costs of financial fraud include: reduced consumer confidence in financial institutions and the financial system as a whole; potential financial and social damage from criminal and terrorist organizations; costs of compliance with industry security measures; inconvenience to customers due to enhanced anti-fraud security measures; a more conservative approach by financial institutions to innovations related to Internet technologies or devices; government spending on fraud is passed on to consumers and financial institutions through higher taxation [13].

The new challenges facing the investigating authorities are related to "identity theft", for the acquisition of which organized criminal groups take advantage of the development of high technology and apply criminal methods such as skimming, phishing, malware, and others. Tackling this type of crime requires constant training and updating of the knowledge of law enforcement agencies and judicial authorities about offline and online fraud.

Therefore, the impact of payment card fraud can be measured in terms of the economic, financial, social, psychological, and moral nature of the adverse effects for each of the stakeholders and for society as a whole. Successful counteraction to the phenomenon requires will and joint efforts on the part of the public sector, business, and civil society structures.

Following meetings, consultations and public discussions at European level, public policy for combating payment card fraud and counterfeiting has received support from stakeholders to introduce clear rules, regulatory framework and mechanisms for the prevention and control of this type of crime after 2000. Despite the diverse interest groups from the three public sectors, a balance has been struck in the process of creating and implementing public policy, stemming from the common interest – security of SEPA payment transactions, dialogue, and good stakeholder interaction.

The products obtained as a result of the implementation of the specific European public policy are related to:

✓ As a form of cybercrime, card payment fraud is one of the priorities of EMPACT (the European Multidisciplinary Platform Against Criminal Threats), Europol's priority criminal areas, within the 2018-2021 EU Policy Cycle for organised and serious international crime [19].

✓ The European policy for combating payment card fraud is based on the Common Strategic Framework as follows: The Council of Europe Convention on Cybercrime of 23 November 2001 [20], the European Union's Internal Security Strategy of 2010 [21], the

European Union Cyber Security Strategy 2020 [22], the European Security Program of 2015 [23] and the Digital Single Market Strategy (COM (2015) 192) of 2015, etc. [24].

✓Creation of regulations from 2000 to 2021 in various areas: harmonized European Internal and Digital Market; protection of personal data; consumer protection; prevention, investigation and prosecution of offline and online payment card fraud; measures against money laundering and terrorist financing; protection of the rights of victims from crime;

✓Institutional capacity building through the establishment of the European Cybercrime Center – EC3 and the European Union Agency for Cybersecurity in the European Union, national cybersecurity units and others. Conducting trainings on offline and online payment card fraud threats;

✓Application of technical standards for protection when performing payment transactions through the EMV standard and partial application of the 3-D Secure protocol in the Member States;

✓Informing and training merchants and cardholders for secure payment transactions by preparing brochures and newsletters from VISA, MasterCard, European ATM Security Team, Europol, EC3, the European Central Bank, the European Banking Authority in order to prevent fraud;

✓Protection of consumer rights, which incl. protection of personal data through legislative (GDPR) and institutional measures;

✓To help consumers the following are created: European Consumer Centers, platforms for alternative and online dispute resolution, mechanisms for rapid notification of loss or theft of payment cards;

✓Conducting investigations and successful international operations by law enforcement agencies in the Member States, Europol, Interpol and the private sector to prevent fraud, destroy organized crime groups and confiscate assets;

✓Criminal prosecution of criminals;

✓Implementation of cooperation between the three public sectors through the establishment of public-private partnerships in expert groups, online platforms between law enforcement agencies and the private sector;

✓International cooperation inside and outside the European Union.

Law enforcement agencies are conducting international actions for combating fraud, as a result of which thousands of compromised cards have been restored and huge losses for the banking sector have been prevented. Investigators are involved in the destruction of organized crime groups and their criminal activities, and confiscate assets. A successful Europol initiative brings together law enforcement and the private sector to tackle payment card fraud in e-commerce. In 2014, at the initiative of the UK authorities, Europol and the European Cybercrime Center supported an 18-month project called Sandpiper, funded by the European Union against payment card fraud. The operation resulted in 59 arrests, 32 prosecutions and 17 convictions, as well as the destruction of five organized crime groups. Investigators are recovering 52,812 compromised payment cards with an expected cost to the banking sector of more than £ 23 million. Based in the European Union, criminals abuse financial powers mainly in remote overseas destinations [25].

European public policies for combating payment card fraud have a favorable effect on the Community by creating a public benefit that translates into political, economic and social benefits for society. The policies provide a secure environment for payment process participants regarding SEPA card-present payments, increasing the security of European consumers and offering additional benefits to non-European citizens operating in the European Union. The technical protection of card-present transactions increases consumer confidence in payment systems, which in turn expands the payment card market by increasing the number of cards and cross-border transactions in the Union. In this way, revenues for traders and financial institutions are also increasing, leading to the development of the Digital

Single Market and to economic growth in the Member States and in the Community. Contemporary payment systems as innovative solutions seek to meet the technological innovations and requirements of the industry. The use of bank cards, e-banking and online payment systems are the most preferred ways to carry out financial transactions by individuals and legal entities. Mobile and contactless payments are one of the most promising areas in the development of e-payments due to convenience, accessibility and time savings. On the other hand, the cost of crime prevention and counteraction measures is high, but responsibility for the costs is shared between the public and private sectors and consumers. In addition, strengthening cooperation between stakeholders in the three public sectors on the prevention and control (sanctions) of payment card fraud will increase the policy efficiency, i.e., to a higher benefit of the policies in the fight against crime with electronic payment instruments and correspondingly lower costs.

In the course of the conducted public policy various challenges from the environment are revealed – external and internal factors regarding: the international character of the payment card fraud; lack of common global security standards; change in consumer behavior by redirecting to mobile and online transactions; increase of card-not-present fraud and losses from them; when transposing European law in the Member States (e.g. Directive 2013/40 / EU on attacks against information systems [26], etc.); in the field of investigation and prosecution (lack of reporting and police statistics on fraud, differences between the units fighting this type of crime in the Member States, etc.); and the large differences in Member States regarding the levels of payment card fraud according to the transaction channel – ATM, POS terminal and no physical presence on the card.

Implementation of the policy for combating payment card fraud in the European Union is related to the harmonization of national legislation and the implementation of measures at regional and national level. European policy is crucial in shaping public policies in the Member States. In addition, it interacts with policies pursued in countries outside the European Union and is implemented in accordance with international norms, global security standards and rules of MasterCard and VISA Inc., in cooperation with Interpol and third countries. Therefore, a common and secure policy on combating payment card fraud in the European Union requires common global standards of security and interaction between stakeholders at national, regional, and international levels.

In their assessments and reports, Europol (The Serious and Organised Crime Threat Assessment – SOCTA and The Internet Organised Crime Threat Assessment – iOCTA) and the European Central Bank make forecasts of future risks and threats, and the corresponding preventive measures in the field of payment card fraud. Skimming devices continue to be perfected through miniature techniques, making them invisible to consumers. At the same time, they are easily accessible and can be purchased freely online [17]. To increase the security of ATMs, several manufacturers of ATMs offer biometric recognition systems. In 2015, the world's first fully functional face and eye recognition system on an ATM device was discovered in China [2].

Cybercriminals don't just attack users to gain access to personal information. Offenders are increasingly turning their attention to service providers, gaining quick access to large amounts of data that they can sell on the black market. This subsequently facilitated an increase in CNP fraud in the European Union [27].

The popularity of mobile and contactless payment technologies will continue to grow in terms of their convenience and accessibility. This will make them an attractive target for criminals looking for a weakness in these technologies. The new risks are: their operating systems are not designed for secure payments; in case of a transaction, the personal data that are missing in other types of payments are exposed to risk; unlike traditional payments, mobile ones include new entrants, incl. mobile network operators; the general public may be less aware of information security when using mobile devices than when paying online from

computers or laptops [28]. On the other hand, their widespread use could lead to a reduction in traditional forms of fraud such as skimmerine, "shoulder surveillance" and others [17].

4 Conclusion

European public policies for combating payment card fraud have a favorable effect on the Community by creating a public benefit that translates into political, economic and social benefits for stakeholders. The policies provide a secure environment for payment process participants regarding SEPA card-present payments, increasing the security of European consumers and offering additional benefits to non-European citizens operating in the European Union. The technical protection of card-present transactions increases consumer confidence in payment systems, which in turn expands the payment card market by increasing the number of cards and cross-border transactions in the Union. In this way, revenues for traders and financial institutions are also increasing, leading to the development of the Digital Single Market and to economic growth in the Member States and in the Community.

On the other hand, the impact of payment card fraud can be measured in terms of the economic, financial, social and psychological nature of the adverse effects for each of the stakeholders. Payment transactions made via the Internet, fax, telephone and mail are subject to higher levels of fraud than traditional payment methods, most of which are made outside SEPA. This causes enormous damage, not only to the International Card Organizations Visa and MasterCard, payment card issuers, but also to airlines, hotels, online merchants and retailers. The cost of crime prevention and counteraction measures is high, but responsibility for the costs is shared between the public and private sectors and consumers.

This type of crime has both economic and non-economic costs. In case of payment card fraud and breach in the systems of banking institutions, their reputation is reduced and the volume of payment transactions is reduced. The feeling of insufficient security and protection leads to distrust and fear in their clients. Tackling this type of crime requires constant training and updating of the knowledge of law enforcement agencies and judicial authorities, private sector and consumers about offline and online fraud.

In the course of the conducted public policy the impact of external and internal factors from the environment is revealed, such as: the international character of the payment card fraud; lack of common global security standards, etc.

Policies for combating payment card fraud and counterfeiting as a type of transnational organized crime require strict measures and joint action between countries on the world stage. Adoption and introduction of uniform technical security standards at global level through EMV technology in "card-present" and strong multifactor identification with 3-D Secure protocol in "card-not-present", on the one hand, and expanding cooperation between the parties, on the other hand, will contribute to a significant reduction in fraud in the European Union and in the world. Continuous interaction between the public, private and civil sectors will favor the implementation of measures in the Member States, reduce payment card fraud in the Union and lead to higher policy benefits and lower costs for stakeholders. Therefore, it is necessary to evaluate periodically the implementation of public policies, for example as conducting ex-post policy impact assessments, including effectiveness and efficiency.

References

1. European Commission, [Towards an integrated European market for card, internet and mobile payments](#) [Green Paper] COM(2011) 941 final, Brussels, 2 (2012)
2. Europol, [The Internet Organised Crime Threat Assessment \(IOCTA\)](#), The Hague, The Netherlands, 33-35 (2015a)

3. Center for the Study of Democracy, Monitoring and Evaluation of Public Policies and Programs, (Sofia, 14, 2009)
4. T. Tomova, *Development of policies, programs, projects*, Handbook for participants in the policy process, Sofia: Bulgarian School of Politics, ISBN 9789549338058, 15, 41, 133, (2008)
5. European Central Bank, Eurosystem, Sixth report on card fraud, (Frankfurt am Main, Germany, 2020)
6. EMVCo, [Worldwide EMV Deployment Statistics. EMV Card-Present Transaction Percentage](#), (2016)
7. European Central Bank, [Guide for the assessment of card payment schemes against the oversight standards](#), Frankfurt am Main, Germany, (online, 2015)
8. Europol, Europol Review – [General Report on Europol Activities](#) 2014, The Hague, The Netherlands, 22, (2015b)
9. Europol, [The Internet Organised Crime Threat Assessment \(iOCTA\) 2016](#), The Hague, The Netherlands, (2016)
10. Verizon, [Data breach investigations report](#), 3 (2014)
11. LexisNexis, [True Cost of Fraud](#)SM, Annual Report, Risk Solutions Retail, 7 (2016)
12. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, (2015)
13. Fr. Burelli, R. Clarke, M. Weston, Ch. Palmer, R. Courtneidge, S. Moore, & V. Lloyd, [Financial Fraud: a Protean Threat](#), (London, UK: Value Partners Management Consulting Ltd. In partnership with Locke Lord, 6-13, 2013)
14. Trud, Growth card payments after the pandemic, (14 February 2021)
15. N. Lee, Credit card fraud will increase due to the Covid pandemic, experts warn, (1 February 2021)
16. L. Fulmer, Payment Card Fraud Losses Reach \$27.85 Billion, (Annual Fraud Statistics Released by The Nilson Report, 21 November 2019)
17. Europol, [The Internet Organised Crime Threat Assessment \(iOCTA\)](#), (The Hague, The Netherlands, 2014)
18. M. Levi & J. Handley, *Criminal Justice and the Future of Payment Card Fraud*. London: Institute for Public Policy Research, 1860301673, 14-24 (2002)
19. Europol, Payment fraud, (2021)
20. Council of Europe Convention on Cybercrime of 23 November 2001, Budapest, 2001, Official Journal 76 (2006)
21. Communication from the Commission to the European Parliament and the Council. EU internal security strategy in action: five steps towards a more secure Europe, European Commission, Brussels, COM(2010) 673 final, (2010)
22. European Union Cybersecurity Strategy 2020, (2020)
23. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Security Agenda, European Commission, Strasbourg, COM(2015) 185 final, (2015)
24. Digital Single Market Strategy (COM(2015) 192), (2015)
25. European ATM Security Team, [EAST releases first European fraud report for 2015](#) [Press release], (27 March 2015)

26. [Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems](#) and replacing Council Framework Decision 2005/222/JHA, Off. J. EU, **L 218/8**, (2013)
27. Europol, [EU Serious and Organised Crime. Threat Assessment](#), SOCTA, (The Hague, The Netherlands, 2013)
28. European Central Bank, Eurosystem, [Third report on card fraud](#), (Frankfurt am Main, Germany, online, 2014)