PROTECTION AGAINST FRAUD IN ELECTRONIC TRADE PAYMENTS

Assoc. Prof. Michal STOJANOV, PhD
University of Economics, Varna
E-mail: michal.stojanov@ue-varna.bg

Abstract: *The past decades have seen continuous advancements of information and communication technologies that have substantially altered economy on a local, national and global scale. The employment of these technologies creates and tranfers to economic entities significant economic and social effects, yet it poses serious challenges to the security of the digital environment. An increasingly complicated issue is that of unlawful activities with payment transactions in trade. This paper reviews the nature of crimes related to payments in the physical and the digital environment; the characteristics of different technological means of safeguarding online payments, as well as some opportunities for improving the safety of individuals when using the Internet to make commercial payments.*

Key words: *electronic payments; security tokens; electronic signature; biometric data; HTTPS.*

JEL: *D18, L81, E42, K14.*

Introduction

Ongoing digital transformation is gradually turning routine daily operations into fully automated processes whose feautures include fast speed, complex service and reduced human errors. One of the challenges to this process is safeguarding the security of digital information. The issue is extremely sensistive in terms of electronic payments, where security requires that payment transactions should be authorized through the adequate authentication of both payers and payees. The authentication process should be easy to accomplish, sparing participants resources, especially time. This implies using upgraded safeguarding mechanisms and tools such as dynamic electronic authentication, electronic signature, the biometric data of payees and data encryption protocols for transmitting data.

The main objective of this paper is to review the characteristics of fraud in electronic payments and the features of various technological devices that are used to safeguard the security of electronic payments in physical and virtual trade environment. To accomplish this, we need to:

1. Summarise and analyse the major theoretical aspects of crimes and safeguarding mechanisms related to electronic payments.

2. Review the most popular instruments for safeguarding electronic payment operations in a digital environment.

3. Analyse financial fraud on a national and global scale, as well as the need to have official information security policies designed by Bulgarian enterprises, and identify opportunities for effective protection against fraud in trade electronic payments.

Contemporary societies and economic entities use multiple payment systems and means of payment, so cash payments are gradually being replaced by non-cash ones. At the same time, in both conventional and digital payment methods dynamic strategies are employed to make sure that the security of payment processes and transactions is adequately guaranteed to all parties involved. In addition, the immense popularity of electronic and mobile trade implies upgrading further the technological devices that are used to protect payments and the personal data of users.

1. Theoretical Aspects of Crime and Safeguarding Electronic Payments

When a payment instrument is issued, its protection is most frequently the responsibility of the issuing entity. Nowadays, however, the commitment to ensure security of payments relates to and is a shared responsibility of all the participants in the payment process. Beside the payment system operator, all users of that payment system may engage in the process of safeguarding it from malicious atempts and contribute to ensuring the more reliable protection of personal data. In addition to security measures like physical security, encripting and data protection tools, the security of modern payments can also be guaranteed by sharing the control over sensitive information. This implies that the parties involved in payment transactions, i.e. payers, payees and intermediaries, can exercise effective control over the authenticity and validity of sensitive data. As a matter of fact, by adding an unpredictable and unique component, any of those parties may add to the security of a payment system and thus exercise personal control over a transaction and the other parties to it. Such decentralization of the payment process will significantly reduce malicious attempts, as they will be rendered inefficient in terms of the other participants in the payment process.

The responsibility of operators and regulators about the performance of official payment systems is essential for efficient consumer protection. This is an underlying principle of Directive (EU) 2015/2366 which implies the wide introduction of personalized security credentials, including ‘an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that

the breach of one does not compromise the reliability of the others, and the procedure is designed in such a way as to protect the confidentiality of the authentication (Direktiva (ES) 2015/2366 na Evropeyskiya parlament i na Saveta na Evropeyskiya sayuz, 2015). The simultaneous or consecutive use of individual security features enhances the security of a transaction and ensures its resilience against unlawful impacts and external attacks. This boosts users' confidence in the payment process and their overall satisfaction with their purchasing experience. Thus, consumers will only be willing to make their purchases online if they feel comfortable and secure in the environment and perceive e-commerce as corresponding to their values and lifestyles (Matsuo & Colomo-Palacios, 2013, p. 118). Obviously, when the security demands of consumers are met, the number of factors that constrain their propensity to engage in trade or increase their consumption will be reduced. In the case of e-commerce, for example, the lack of risks related to payments may encourage consumers to spend more time and to pay more attention to the other elements of their purchasing experience. The Bulgarian Criminal Code (Nakazatelen kodeks, 2017), determines theft as taking away from another movable property without his content, with the intent to unlawfully appropriate (Section One of the Criminal Code), whereas deceit is defined as causing a material damage by taking advantage of a misleading idea, the inexperience or the lack of information of another (Section Four of the Criminal Code). Those two crimes against property relate to purposeful actions for the misappropriation of property in an unlawful manner by the offender. A theft implies causing material damages to another without the knowledge of the owner, whereas in the case of deceit, owners are purposefully led to a situation in which unfavourable effects result from their own actions due a misleading idea which the offender has evoked or maintained. Typical examples of such crimes committed in the sphere of trade include consumers who become victims of data theft when using non-cash payment instruments or sharing information about customers when they do their online shopping on fake web pages that mimic companies with established market image and reputation.

Crimes committed against the monetary and credit system are treated as a separate group of crimes. They are qualified as producing false or forging genuine bank notes and coins or payment instruments (Art. 243 of the Criminal Code). Such crimes also relate to deliberately compromising the security features that protect the integrity of the means of payment. They are further specified as 'using an instrument of payment or data from an instrument of payment without the consent by the holder thereof' (Art. 249 of the Criminal Code). The preparation, installment or making use of a technical facility in order to obtain information about the contents of an instrument of payment is also treated as a crime (Art. 249 of the Criminal Code). This implies that any unlawful and deliberate attempt to access sensitive information which results in negative economic effects qualifies as an economic crime. This relates directly to modern non-cash means of payment that are gradually replacing traditional means of payments in trade. Hence, the scope of prosecution has been expanding, too, in order to respond adequately to the digital transformation of economic processes.

As for the use of computer and information systems, offenses relate mainly to the unlawful access and use of computer data in one or more computer systems (Chapter Nine 'A' of the Criminal Code). The seriousness of offense is also determined by the extent of harmful effects or other major damages resulting from the unathorised interference into the operation of computer systems and networks. The normal operation of remote computer systems and networks requires the use of telecommunication networks, therefore Art. 348a of the Criminal Code defines as a crime the deceit and any other unlawful means that make use of telecommunication networks, equipment or services in order to unlawfully generate or transmit messages in the transmission environment. Therefore, any unlawful interference in the electronic data transmission environment, including in terms of electronic payment transactions, is a legally prosecutable offense.

In addition to the Criminal Code, there are provisions against crimes related to payments and the use of means of payments in other regulations, such as the Law on Payment Services and Payment Systems, the Electronic Communications Act, the Consumer Protection Act, the Law on Credit Institutions, the Law for Protection of Personal Data, etc. Hence, the legislator has foreseen a number of hypotheses related to deliberate frauds in making trade electronic payments. The parties involved in the payment process thus have a number of reliable tools to protect their transactions, in addition to the mechanisms designed for prosecuting and sanctioning unscrupulous behavior. A relevant example is the right of consumers to withdraw from a distance contract or from an off-the premises contract without giving any reason, without having to pay compensation or penalty and without bearing any costs whatsoever other than the cost of delivery within a period of 14 days (Art. 50 of the Consumer Protection Act) (Zakon za zashtita na potrebitelite, 2018). Such provisions are also made in the EU General Data Protection Regulation (GDPR or Regulation (EU) 2016/679) that sets stricter requirements to the regulation of personal data privacy. According to that Regulation,'effective protection of personal data requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements' (Reglament (ES) 2016/679 na Evropeyskiya parlament i na Saveta na Evropa, 2016). This implies that any processing of personal data shall be in compliance with the existing laws and shall be conducted for purposes that have been strictily defined and are known to the parties, with the agreement of the data subject or resulting from legal regulation, ensuring transparency and providing data subjects with legally enforceable rights, etc. The mandatory nature of the EU General Data Protection Regulation (GDPR) within the EU will cause dramatic changes in all business spheres, including in the manner in which commercial companies collect and process data about their customers, and above all, the protection of such data. Bulgarian legislation also prohibits the misuse of 'production or trade

secrets that are defined as facts, information, decisions or data related to economic activities, the preservation of confidentiality of which is in the interest of the rightful holders thereof' (§1 p. 9 of the Law on Protection of Competition). This provision is also applicable to actions which are not in compliance with good commercial practices; may lead to unfavourable economic or other consequences of the unlawful acquisition, use or disclosure of facts and knowledge protected by a company. Such information may relate to internal business processes as well as to the external micro-environment of entities. This is primarily the information which an economic entity processes as a data controller. Hence the focus on the requirement that business entities which exchange or have access to such information must plan and employ adequate measures to protect it. Within this context, disloyal behaviour between business partners or competitors, may be sanctioned by the Commission for Protection of Competition when a request is submitted, after initiating relevant proceedings, conducting an investigation and adopting a decision about an infringement that has been established and proven. Those examples confirm that there could be various hypothetical situations in which the interests of the parties involved in electronic payments might be directly or indirectly infringed.

The different types of fraud in electronic transactions may be classified according to numerous criteria which are presented in brief in the table below (Table 1).

Table 1
Classification of the types of fraud in electronic payment transactions

Classification criteria	Types of fraud
According to their spread in an electronic environment (Juniper Research, 2016, pp. 13-15)	• Clean fraud; • Account takeover; • Friendly fraud - when a merchant receives a chargeback because the cardholder denies making the purchase or receiving the order, yet the goods or services were actually received; • Identity fraud; • Affiliate fraud; • Re-shipping – a deceitful scheme for re-shipping unlawufully acquired assets by recruiting an informed or innocent person, known as a 'mule'; • Botnets – networks and/or malware which operate in a stand-alone mode and aim at personal data theft; • Phishing attacks relate to the use of fraudulent web sites or receiving deceitful electronic communications disguised as 'warnings from banks or other entities the consumer interacts with' (Gaydarov, 2018); • Whaling, or spear phishing, is phishing targeted on certain individuals; • Pharming is re-directing web-site traffic to an illegal site where customers unknowingly enter their personal data; • Triangulation is stealing debit and credit cards credentials trough on-line auctions, ticketing sites or online classified ads. of tickets and online ads.

According to the type of threats/attacks in terms of payments (European Payments Council, 2018)	• Distributed Denial of Service (D)DoS); • Social engineering); • Phishing; • Malware; • Advanced Persistent Threats (APTs); • Mobile device related attacks; • Botnets; • Threats related to cloud services and big data; • Threats related to the Internet of Things (IoT); • Threats related to virtual currencies; • Deceits related to payment cards; • Deceits related to automated teller machines (cashpoints).
According to the stage of the commercial transaction which is affected by the fraud	• Before the sale: counterfeit traders, unrealistic trading conditions,misleading information, etc.; • During the sale: frauds with credit card and means of payment upon the purchase of the product, changing the terms of the deal, etc.; • After the sale: frauds related to the delivery, frauds related to the product return, etc.
According to the territorial scope and the victims of the fraud (Kratcoski, Dobovsek, & Edelbacher, 2015, p. 30)	• Domestic (national) • International
According to who the fraud is targeted on (Dalla & Geeta, 2013)	• Against personality • Against property • Against the state • Against society
According to the victim of fraud (Bernard, et al., 2017, p. 14)	• Against physical entities / citizens • Against legal entities / businesses and organsiations
According to the seriousness of Art. 49, p. 7, 8 and 9 of the Criminal Code (Nakazatelen kodeks, 2017)	• A 'Minor case' is that in which the crime perpetrated, in view of the lack of or insignificance of the harmful consequences, or in view of other attenuating circumstances, constitutes a lower degree of social danger, as compared with ordinary crime cases of the respective kind; • A 'Grave crime' is any crime for which the law provides punishment by imprisonment for more than five years, life imprisonment or life imprisonment without substitution; • A 'Particularly grave case' is that in which the crime perpetrated, in view of the harmful consequences that have occurred and of other aggravating circumstances, reveals extremely high degree of social danger of the act and the perpetrator

The more general and specific criteria listed in the table above are evidence of the extremely complex and constantly changing nature of fraud in electronic payments, which requires that counteractive measures should be regularly updated. This could be achieved by constantly monitoring and updating organizational and technological means and safeguards for preventing fraud in electronic payments in e-commerce.

2. Safeguarding Instruments for Online Payments

Any payment transaction which is defined as 'an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee' (Dopalnitelni razporedbi na Zakona za platezhnite uslugi i platezhnite sistemi, 2017), must be secured with some level of protection. The participants in cash payment transactions are able to exercise total control on the site where a payment is made through a physical inspection. Such an inspection is made through the manual or automated verification of the high-tech security features which are built-in in modern payment facilities. In contrast, in the case of electronic payment operations and especially those which are conducted entirely in an electronic environment, safeguarding mechanisms require adequate digital innovations and additional control and security mechanisms.

This part of the article reviews some of the most popular technological solutions which are currently used to safeguard non-cash payments, as well as some opportunities for their further development:

• Using a safeguarding https (HyperText Transfer Protocol Secure) protocol to transfer data on the internet. To enhance security, a connection between end users and the web server of a retailer is established to transfer encrypted communications. The protocol encrypts any data sent over the global network so that only pre-identified participants in the data-exchange process will be able to read them. Sensitive user data as well as consumer behavior online can be protected against malicious and unauthorized monitoring and manipulation. The identity of the parties is confirmed with an SSL (Secure Socket Layer) certificate which is added to the data transfer protocol allowing only the end users in the online communications exchange to establish a secure connection that is protected against unauthorized interception. This raises the digital trust of e-customers in their partners in the communication exchange who ensure a reliable environment for transferring information. One of the benefits of this mechanism is that it is secondary to the process of internet communication, so online users do not engage in its automated operation. Consumers can thus focus on their e-shopping experience, yet they could check the security of the connection, the identity of the certificate and the reliability of the organization that identifies the retailer through their domain or web-site. According to W3Techs (Gelbmann, 2018), the most popular SSL

certificate authorities for websites at the end of 2017 were Comodo, IdenTrust and DigiCert Group. Modern applications for browsing the internet thus ensure a relatively secure environment for online shopping experiences, regardless of the operating system or the hardware which is used. This enables customers to focus on products, their features and the terms of sale without being distracted by factors such as an insecure payment or the risks related to the use of personal data. Another option is the use of an SET (Secure Electronic Transactions) protocol which limits the access of customers, retailers and payment institutions to sensitive data about the virtual means of payment to what they really need. A major feature of the operation of that mechanism is the primary role and engagement of payment systems operators, which renders the mechanism more difficult to use and hence reduces its popularity in real e-commerce, compared to the SSL protokol.

• Security tokens. Those are special miniature devices that can receive, store and send digital codes in order to authorize certain opeartions. Various components may be added to enable them to communicate with other devices and systems or to visualize authorization codes (keys). These are provided to payees by their payment service providers to authorize the remote electronic payment for products purchased online. Token devices can generate unique identification codes that may be used as one-time passwords or for limited periods of time, their limited service life thus increasing the security they offer. Security tokens are an upgraded variety of traditional security methods that include payers' personal data. Thus, in addition to the static combination of letters, digits and symbols which users enter to verify payments, an additional static or dynamic code is provided or transferred by the payment system operator or the payment services institution. Such codes could be sent to users who prefer them to special token devices via alternative communication channels like an e-mail, an SMS from a mobile communications operator, etc. Modern smart telecommunication devices can thus emulate both classic bank cards and security tokens so that they become a major element of secure payments in physical and virtual trade. What is more, their use does not require the time or attention of users once they are attached to the user interface of the hardware that is used to make a payment. A physical connection between devices is not necessary even for near-field communication (NFC).

• Electronic signatures. Those are 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication' (Direktiva 1999/93/EO na Evropeyskiya Parlament i na Saveta na Evropa, 2000) and which may be used by the signatory to sign documents (Reglament (ES) No. 910/2014 na Evropeyskiya parlament i na Saveta na Evropa, 2014). An electronic signature is therefore an instrument for communicating information securely by guaranteeing the authenticity, integrity, confidentiality and irrevocability of the statements made by the holder of an electronic signature when engaging in specific electornic operations and activities in an electronic environment. Parties may stipulate to consider the value of an electronic signature attached to any electronic statement equal to a hand

signature in the relations between them. According to Art. 13 of the Law for the Electronic Document and Electornic Certification Services (Zakon za elektronniya dokument i elektronnite udostoveritelni uslugi (title amended in SG 85/2017), 2017). The use of electronic signatures makes it possible to widen the range of remote commercial transactions and meet the requirement about the mandatory formalization of purchases and sales. The power and consequences of using an electronic signature equal those of personal statements which are actually signed. At the same time the benefits of using electronic signatures also relate to their publicity, since they may be verified by the recipients of documents.

• Biometric data. Modern smart devices (computers, telecommunication devices, etc.) are increasingly being configured with components that enable users to identify themselves by using biometric data. According to the Bulgarian Identity Documents Act, biometric data are defined as 'the image of the citizens' face and his/her fingerprints which shall be used for recognition and verification of the stated identity' (Zakon za balgarskite lichni dokumenti (title amended in SG 82/2009), 2017). Users can thus identify themselves by using their unique physical features. The identity of consumers can be unambiguously confirmed in purchase and payment activities by using their fingerprints (i.e. through dactyloscopy) and/or their facial, voice or other biometric recognition. Biometric authentication ensures the highest level of protection on sale sites and in payment transactions. The technology of using biometric data for authentication implies more serious safeguarding mechanisms both in terms of employed algorythms and devices and in comparison to other alternatives for ensuring the security of payments. What is more, the use of biometric technologies is of benefit to all parties since it 'improves the shopping experience and guarantees the security of the payment' (Perez, 2018), wherever the point of sale is. The latter makes possible the optimization of the payment process in several aspects, and above all in terms of its security and the time required to make the payment. The opportunities for using biometric data in electronic and mobile commerce are numerous due to the cameras, microphones, and even fingerprint readers which modern laptops, tablets, smart phones, etc. have built in. Biometric authentication in electornic and mobile commerce thus optimizes the final stage of the process of exchange, that is, making a digital transaction. Issues related to security, eliminating potential risks along the payment chain and guaranteeing the comprehensive protection of the parties involved in the payment process are extremely important at that stage. Biometric authorization and authentication help establish the identity of customers in electronic and mobile commerce payments by creating a safeguarding virtual bridge between the web page of the retailer or the provider of payment services and the payer, in compliance with the provisions of Directive (EU) 2015/2366. Biometric authentication may be employed in all varieties of retail trade provided that the point of sale has the necessary equipment; the staff has the skills and competence required for using that equipment and customers are familiar with the technology as well.

These solutions are some of the mechanisms that may be employed to check the identity of customers and their operations when making electronic payments in a real and a virtual environment where thefts, frauds and malicious activities may be attempted by third parties. Their focus is on guaranteeing the security of payment services through the authentication of parties involved in them. The mechanisms through which these solutions operate guarantee that before, at the time of and after a payment operation, regardless of the location or the time when the payment is made, records will be made so that the identity of all participants in the payment process could be established and related data and cash flows could be tracked.

Furthermore, identification and authentication are the up-to-date approach to combating the risk of fraud in trade payments. As a matter of fact, the greater the number of the levels of protection and the shorter the time of the authentication processes, the higher the satisfaction of all parties involved and the security of their payment accounts will be.

Employing various instruments to safeguard payment operations in an electronic environment requires that the parties involved in such payments (as the receivers of sensitive data) and the persons who can access and view such data should be granted relevant access rights and authorization to process data, while their activity should be efficiently safeguarded. All these factors determine the role of data administrators and their rights and responsibilities in terms of operations related to electronic payments. Hence, both the infrastructure used to transfer payment operations data and the devices used to access and work with payment operations systems need to be further protected. To do this, modern technological solutions are employed in addition to the established organization of electronic payment operations. Firewalls are the most popular technological solution. Firewalls can be implemented as hardware or software or a combination of both and ensure the continuous automated inspection of incoming and outgoing network traffic to and from electronic payment systems. The key function of any firewall is to monitor and inspect data transfer based on a defined set of security rules and decide whether to allow or block incoming or outgoing network traffic. Physical entities who have access to terminals that are part of electronic payment systems might be required to present certificates of non-conviction when applying for a job, in compliance with Art. 1 (1) p. 5, Ordinance No. 4 on the documents required for signing a contract of employment (Ministerstvo na truda i sotsialnita politika, 2017). Organisations will thus be equipped with a preventive tool they may employ when appointing employees who will have access to and work with electronic payment systems. It would also be appropriate to implement a two-factor or multi-factor authentication policy for operations conducted with terminals of the electronic payment systems. This could be achieved with U2F (Universal 2nd Factor) personal devices for all users who have access rights. Another standard that is additionally introduced is restricting the access to certain elements of the system outside specific locations and according to certain rules. Remote access is made possible by using a suitable tunneling protocol

for working in a virtual private network, such as PPTP, L2TP, OpenVPN, SSTP, IKEv2 (Fouks, 2016). All these solutions ensure a higher level of protection and control over the access to the electronic payments systems and when using personal data about the people involved in online commerce.

3. Challenges to Safeguarding Online Payments in Trade

The evolution of payment systems and accompanying innovations in technoilogies contribute to improved trading conditions and the transfer of commerce into the digital environment. The application of artificial intelligence makes it possible to gain benefits in terms of protection from fraud in sales, too. Intelligent and automated analytical systems constantly monitor user activity and can implement real-time corrective actions; detect new unfamiliar schemes of fraud in online trade and payments. Machine learning, combined with artificial intelligence, can offer solutions to make the process of trading more efficient both economically and socially. Machine learning applications are deployed to improve the supply chain, to study consumer behavior and to combat fraud in trade transactions. The latter usually relate to financial fraud which has become pandemic around the world. Thus in 2016, the number of victims of financial fraud in the USA alone was 15.4 million people, with an annual increase of 16% and an equivalent of US $ 16 billion, which is an annual increase of nearly US $ 1 billion (Miller, Marchini, & Pascual, 2017). Card fraud losses in Europe in 2016 hit nearly 1.8 billion euros, the UK and France accounting for almost three-quarters of card fraud across Europe (Ecommerce news, 2017). This explains why concern about fraud is the primary barrier to online payments for half of the European online shoppers (Masterindex 2017, 2017, p. 7). In the Republic of Bulgaria, the total number of crimes against the property in 2017 was 5,882; 65.1 % of them (i.e. 3,827) were classified as theft; 10.6% (or 623) were classified as robbery, in addition to 377 crimes against the monetary and credit system over the same period (Natsionalen statisticheski institut, 2018). In comparison, seven years earlier, that is, in 2010, the number of reported thefts was 8,973 and that of reported robberies – 1,114, the total number of reported crimes against the property being 12,538 and that of crimes against the monetary and credit system – 257. The reduction in the number of crimes against the property by 6,656 (i.e. by 53%) was accompanied by a 146.7% growth in the number of crimes against the monetary and credit system. There was a positive trend in terms of the problems encountered by Bulgarian citizens when buying or ordering goods over the internet, too. The relative share of individuals who were victims of fraud was 0.3% in 2017, in contrast to 2.9% in 2004 (Natsionalen statisticheski institut, 2017). The number of individuals who fell victim to fraud when making purchases on the internet was the biggest in 2006, when 3.7% of Bulgarians who engaged in an online shopping activity reported that they had been negatively affected by e-

commerce fraud. Globally, according to the ciber crimes reported to the Internet Crime Complaint Center of the USA Federal Bureau of Investigation, victim losses were the highest in 2016 (US $1,450.7 million), the value of losses reported in 2017 being US $1,418.7 million (Federal Bureau of Investigation, 2018, p. 4). Compared to the year 2001, when losses from ciber crimes amounted to only US $ 17.8 million, this was a 79-fold increase (The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation, 2008, p. 3). Ciber crime is therefore becoming a global problem. 'In the EU, more than a tenth of all internet users have already been victims of online fraud' (Evropeyska Komisiya, 2013, p. 3). At the same time, we need to emphasise three major issues in terms of public information and the real size of crime in e-commerce payments. The first one is that a substantial share of the instances of fraud in digital payments are not reported or registered. The second issue is that the share of fraud cases that are not officially reported due to the provisionally insubstantial material damage that has been caused, is significant. The third problem is that the improvement of safeguarding systems is lagging behind the development of organized crime. This is mainly due to the limited resources available for regular software and hardware updates. The new reality demands alternative methods for combating fraud, which has led to the design of a new type of electronic services to safeguard data used in digital payments in commerce. At the same time, users can increase the security of their online payments themselves by following some of the most popular recommendations for combatting fraudulent attempts (GDBOP-MVR, 2018). Those include:

• Informing the payment institution which handles the user's payment accounts that they have been subject to fraudulent activity. Provided that users contact their payment institution promptly and give comprehensive information about the suspicious activity, standard protocoles designed to safeguard the interests of users and the payment institution are activated.

• Informing the payment institution and data protection authorities when establishing that their personal data and documents which are directly or indirectly related to payment instruments have been subject to theft.

• Regularly monitoring movements on their payment accounts, requesting electronic notification by e-mail or an SMS from mobile operators about active payment operations that have been attempted and/or made from their accounts. When unsolicited payments or unusual transactions are registered by account holders, they need to request detailed information from their payment institution, insist on adequate coorective actions or submit a chargeback claim.

• When any misuse or unusal activity from a user account with an online merchant is established, account holders should send a notification that their user account or profile has been compromised. Upgraded ecommerce platforms have an option that enables buyers to monitor their account activity and sessions. Should users identify any unusual activity, they can inform the

platform administrator or upgrade their log-in and information retrieval protection. Users can use their accounts with a specific merchant for a particular transaction only or for a specified number of transations. Users can also decide that they no longer want to make purchases from an electronic merchant. In that case, pursuant with Art. 17 of Regulation (EU) 2016/679, the customer (data subject) has the right 'to be forgotten'. This provision becomes mandatory and should be directly implemented in the economic and social activity of any member-state as of 25th May 2018. According to Regulation (EU) 2016/679, a user 'shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay since they are no longer needed for the purposes for which they have been collected' (Reglament (ES) 2016/679 na Evropeyskiya parlament i na Saveta na Evropa). Hence, all agents engaged in online commerce are obliged to design a corporate policy to effectively and lawfully protect the personal data of EU citizens which they collect and use in their business activity, regardless of the geographical location where their company is registered. Thus, protecting the rights of EU consumers becomes a mandatory obligation.

• Online users should take care and upgrade the security of the operational systems at least by installing the right software that will protect their computer configuration from malware. Upgrading to the latest versions of the protection software and the malware detection libraries which they use can, to a certain extent, limit the risk exposure. This also implies that users should regularly update their browsers. At the same time, internet users need to continuously expand their culture and knowledge about the services provided in the information society, so that they could adequately meet the challenges posed by the processes of digital transformation and evolution. The European Payments Council gives a number of recommendations for effectively controlling and mitigating the impact of payment security threats in the annual reports it publishes. The major findings of the Council in terms of common threats in the payments landscape relate to: 'a greater degree of professionalism of cybercriminals; a growing number of Distributed Denial of Service (D)DoS) attacks and their frequent targeting the financial sector; a shift in the attack focus from malware to social engineering attacks; a shift of attacks from customers, retailers and SMEs to company executives, employees, financial institutions and payment infrastructures; malware and especially ransomware (software used to hack into computer systems and demand the payment of a ransom) remaining a major threat; a continuation of botnets because of the high volume of infected consumer devices; multi-vector attacks which target mainly financial institutions; mobile devices becoming an increasingly attractive target for cyber criminals, along with the Internet of Things devices; the adoption of cloud services and big data analytics which results in data stored 'everywhere', thus bringing new opportunities to businesses, but new risks, too' (European Payments Council, 2017, p. 5). Another

phenomenon that is appearing is ‘cybercrime-as-a-service’ (European Payments Council, 2018, p. 6), which makes possible the development of an alternative market for similar malicious services with specific and highly profiled supply and demand.

Another issue to be considered in terms of online payment fraud is that of information. This problem is common to all participants in cashless payment systems due to the lack of sufficient knowledge and awareness about the growing variety of fraud schemes and new ciber crimes. In some cases, part of the information that has been gathered at some stage of crime investigation is not disclosed so that the primary sources of malicious activity could be identified. This often results in the delayed response of the parties affected by such actions. That is why the European Commission points out that ‘ensuring cybersecurity is a common responsibility’ (Evropeyska Komisiya, 2013, p. 9) where end users play a crucial role in ensuring the security of online payments. This implies cultivating in all users the skills and digital literacy required for making safe online payments.

These are some aspects of consumer protection in both physical and virtual environment. Business agents can also employ information security tools and implement security policies. The findings of a survey conducted in 2010 in Bulgarian enterprises about the information and communication technologies they employ in their activity indicate that only 6.8% of the companies in the country have adopted a formal information security policy (see Fig. 1) (INFOSTAT - Natsionalen statisticheski institut, 2018). Five years later, in 2015, nearly one out of five companies (18.6%) had adopted a formal approach for effectively safeguarding sensitive information. Despite the recorded increase of more than 274%, the level of adoption of information security policies was still far below the average for the EU-28, that was 28% in 2015 (Eurostat, 2018). Significant progress was made in larger economic entities where the number of employees is more than 250 people. More than half of them, i.e. 54.5% of those enterprises, had a formally designed ICT security policy. Small enterprises (with employees from 10 to 49 people) are lagging far behind – only 5.45 of them took any actions to manage their information security in 2010, the share rising to 15.4% in 2015.

The process will undoubtedly be accelerated by Regulation (EU) 2016/679 which refers to all natural or legal persons that collect or process personal data about natural persons to conduct their economic activity. Entities will thus be obliged to design adequate policies which are in compliance with legal requirements on personal data protection and ICT security. Such an approach clearly defines the responsibilities and enagements of the entities that have access to personal data, as well as the measures that need to be adopted in order to align and secure personal data processing in enterprises and guarantee the fundamental rights of EU citizens.

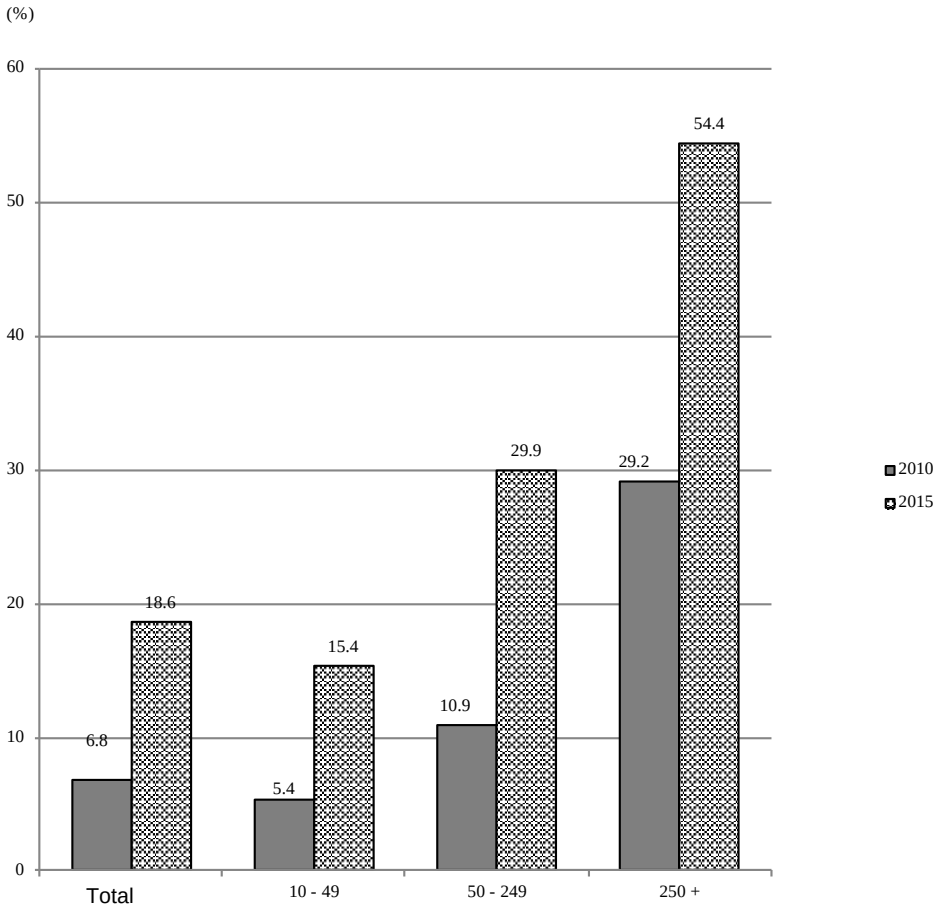

Figure 1. Enterprises in Bulgaria that had a formally designed policy for ICT security in 2010 and in 2015 (as a percentage)
Source: NSI (ICT usage in enterprises).

Conclusion

At present, there is no universal or comprehensive approach to protect users against e-commerce fraud, yet, the more efficient the cooperation between merchants and customers, the lower the risk of malicious attacks. In addition, users should not assume that all the other participants in physical and virtual commerce act in good faith, but need to take on their own responsibility for protecting their personal data and payment instruments when using online payment services and systems.

References

Bernard, B., Johnson, H. H., Hodgson, H., Mills, L., Coates, S., Turner, H., etc. (2017). *Online fraud.* National Audit Office. London: National Audit Office Press Office.

Dalla, E. H., & Geeta, M. (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 997-1002.

Direktiva (ES) 2015/2366 na Evropeyskiya parlament i na Saveta na Evropeyskiya sayuz. (23 dekemvri 2015). Direktiva (ES) 2015/2366 ot 25 noemvri 2015 godina za platezhnite uslugi vav vatreshniya pazar, za izmenenie na direktivi 2002/65/EO, 2009/110/EO i 2013/36/ES i Reglament (ES) No. 1093/2010 i za otmyana na Direktiva 2007/64/. Ofitsialen vestnik na Evropeyskiya sayuz, OJ L 337, 35-127 [In English: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC/.Official Journal of the European Union]

Direktiva 1999/93/EO na Evropeyskiya Parlament i na Saveta na Evropa. (19 01 2000). Direktiva 1999/93/EO ot 13 dekemvri 1999 godina otnosno pravnata ramka na Obshtnostta za elektronnite podpisi (otmenena). *Ofitsialen vestnik na Evropeyskiya sayuz OJ L 13, Special edition in Bulgarian: Chapter 13, Volume 028*, pp. 12-20 pp. 120-129. [In English: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (repealed). *Official Journal of the European Union*]

Dopalnitelni razporedbi na Zakona za platezhnite uslugi i platezhnite sistemi. (2017). *Obn. DV. br.23 ot 27 Mart 2009g., posl. izm. DV. br.97 ot 5 Dekemvri 2017g.* [In English: Additional Provisions of the Law on Payment Services and Payment Systems. *Prom. SG. 23/27.03.2009, last amend. SG 97/05.12.2017.]*

Ecommerce news. (29.06.2017). *UK and France account for 73% of European card fraud.* Retrieved on 30. 01. 2018 from Ecommerce News: https://ecommercenews.eu/uk-france-account-73-european-card-fraud/

European Payments Council. (2017). *2017 Payment Threats and Fraud Trends Report.* Brussels: Conseil Européen des Paiements AISBL.

European Payments Council. (2018). *2018 Payment Threats ans Fraud Trends Report.* Brussels: Conseil Européen des Paiements AISBL.

Eurostat. (2018). *Enterprises had a formally defined ICT security policy.* Retrieved on a 08.02.2018 from ICT usage in enterprises (isoc_e): http://ec.europa.eu/eurostat/data/database

Evropeyska Komisiya. (2013). Savmestno saobshtenie do Evropeyskiya Parlament, Saveta, Evropeyskiya ikonomicheski i sotsialen komitet i

Komiteta na regionite. Strategiya na Evropeyskiya sayuz za kibersigurnost. Otvoreno, bezopasno i sigurno kiberprostranstvo. Bryuksel: EUR-Lex - 52013JC0001 - BG - Sluzhbata za publikatsii na ES. [In English: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: EUR-Lex - 52013JC0001 - BG - The Publications Office of the EU.]

Federal Bureau of Investigation. (2018). *Internet crime report 2017.* Internet Crime Complaint Center.

Fouks, G. (11 Noemvri 2016 r.). *Sravnenie na VPN protokoli: PPTP – L2TP – OpenVPN – SSTP – IKEv2.* Retrieved on 23 January 2019 from vpnMentor: https://bg.vpnmentor.com/blog/vpn-protocol-comparison-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

Gaydarov, I. (27 June 2018). *Kak da izbegnem fishing izmami?* Retrieved on 28 January 2019 from PC World: https://pcworld.bg/polezno/2018/06/27/3211156_Как да избегнем фишинг измами%3F/

GDBOP-MVR. (2018). *Zaplahi v Internet*. Retrieved on 31 01 2018 from Ofitsialen sayt za borba s kompyutarnite prestapleniya: http://www.cybercrime.bg/bg/internet/

Gelbmann, M. (03 01 2018). *Web Technologies of the Year 2017.* Retrieved on 30.01.2018 from W3Techs: https://w3techs.com/blog/entry/web_technologies_of_the_year_2017 and https://w3techs.com/technologies/overview/ssl_certificate/all

INFOSTAT - Natsionalen statisticheski institut. (2018). *Predpriyatiya, koito imat ofitsialna politika za informatsionna sigurnost*. [In English: INFOSTAT - National Statistical Institute. *Entreprises Having a Formally Defined ICT Security Policy*]. Retrieved on 28. 02.2018 from https://infostat.nsi.bg/infostat/pages/reports/query.jsf?x_2=1365

Juniper Research. (2016). *Online payment fraud whitepaper 2016-2020.* Basingstoke, Hampshire, United Kingdom: Juniper.

Kratcoski, P., Dobovsek, B., & Edelbacher, M. (2015). *Corruption, Fraud, Organized Crime, and the Shadow Economy.* Boca Raton, FL: CRC Press.

Masterindex 2017. (03.2017). *Pan-European e-commerce and new payment trends.* Retrieved on 30.01.2018 from https://newsroom.mastercard.com/wp-content/uploads/2017/03/Masterindex-2017.pdf

Matsuo, T., & Colomo-Palacios, R. (2013). *Electronic business and marketing: New trends on its process and applications.* SCI 484, Springer – Verlag Berlin Heidelberg.

Miller, S., Marchini, K., & Pascual, A. (01 02 2017). *2017 Identity Fraud: Securing the Connected Life.* Retrieved on 29.01.2018 from dba as Javelin Strategy & Research: javelinstrategy.com

Ministerstvo na truda i sotsialnita politika [In English: Ministry of Labour and Social Policy]. (2017). Naredba No. 4 za dokumentite, koito sa neobhodimi za sklyuchvane na trudov dogovor. Izdadena ot ministara na truda i sotsialnata politika. *Obn. DV. br.44 ot 25 May 1993g., izm. i dop. DV. br.99 ot 12 Dekemvri 2017g*.

Nakazatelen kodeks. [In English: The Criminal Code].(2017). Obn. DV. br. 26 ot 2 April 1968 g., posl. izm. i dop. DV. br. 101 ot 19 Dekemvri 2017 g.

Natsionalen statisticheski institut. (8 dekemvri 2017 g.). Problemi, sreshtani pri porachki ili pokupki na stoki i uslugi prez internet. [In English: National Statistical Institute. (8th December 2017). *Problems encountered when buying/ordering goods or services over the Internet*]. Retrieved on 28 January 2019 from NSI: http://www.nsi.bg/sites/default/files/files/data/timeseries/ICT_HH_1.2.4.xls

Natsionalen statisticheski institut. (16 yuli 2018 g.). Prestapleniya po glavi ot nakazatelniya kodeks i nyakoi vidove prestapleniya i po izhod na delata. [In English: National Statistical Institute. (16th July 2018). *Crimes by chapters of penal code and some kind of crimes and according to results of proceedings*.] Retrieved on 23 January 2019 from NSI: http://www.nsi.bg/sites/default/files/files/data/timeseries/JST_1.3.xls

Perez, J. (22 01 2018). *Mastercard establishes biometrics as the new normal for safer online shopping.* Retrieved on 28.01.2018 from Mastercard Press Releases: https://newsroom.mastercard.com/eu/press-releases/mastercard-establishes-biometrics-as-the-new-normal-for-safer-online-shopping/

Reglament (ES) 2016/679 na Evropeyskiya parlament i na Saveta na Evropa. (04 05 2016). Reglament (ES) 2016/679 ot 27 april 2016 godina otnosno zashtitata na fizicheskite litsa vav vrazka s obrabotvaneto na lichni danni i otnosno svobodnoto dvizhenie na takiva danni i za otmyana na Direktiva 95/46/EO (Obsht reglament otnosno zashtitata na dannite). *Ofitsialen vestnik na Evropeyskiya sayuz*, *OJ L 119*, pp. 1-88. [In English: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, OJ L 119*, pp. 1-88.]

Reglament (ES) No. 910/2014 na Evropeyskiya parlament i na Saveta na Evropa. (28 08 2014 r.). Reglament (ES) № 910/2014 ot 23 yuli 2014 godina otnosno elektronnata identifikatsiya i udostoveritelnite uslugi pri elektronni transaktsii na vatreshniya pazar i za otmyana na Direktiva 1999/93/EO. Ofitsialen vestnik na Evropeyskiya sayuz OJ L 257, pp. 73-114. [In English: REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in

the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union OJ L 257*, pp. 73-114]

The National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation. (2008). *Internet crime report 2007.* Cybercrime reported to IC3.

Zakon za balgarskite lichni dokumenti (zagl. izm. - DV, br. 82 ot 2009 g.). (2017). *Obn. DV. br. 93 ot 11 Avgust 1998 g., posl. izm. DV. br. 97 ot 5 Dekemvri 2017 g.* [In English: Bulgarian Identity Documents Act (title amend. - SG, 82/2009). (2017). *Prom. SG 93/11.08.1998, last amend. SG 97/05.12.2017*]

Zakon za elektronniya dokument i elektronnite udostoveritelni uslugi (zagl. izm. - dv, br. 85 ot 2017 g.). (2017). *Obn. DV. br. 34 ot 6 April 2001 g., posl. izm. i dop. DV. br. 85 ot 24 Oktomvri 2017 g.* [In English: Electronic Document and Electornic Certification Services Act (tiltle amend. - SG 85/2017). Prom. SG 34/06.04. 2001, last amend. and suppl. 85/24.10.2017.]

Zakon za zashtita na potrebitelite. (2018). Obn. DV. br. 99 ot 9 Dekemvri 2005 g., posl. izm. DV. br.7 ot 19 Yanuari 2018g. [In English: Consumer Protection Act. (2018), Prom. SG 99/09.12. 2005, last amend. SG 7/19.01.2018.]

D. A. Tsenov Academy of Economics, Svishtov
University of National and World Economy, Sofia
University of Economics, Varna
Sofia University St. Kliment Ohridski
New Bulgarian University, Sofia

ECONOMICS 21

An inter-university scientific journal
Volume IX, Issue 1, 2019

TABLE OF CONTENTS

ECONOMICS 21

AN INTER-UNIVERSITY SCIENTIFIC JOURNAL

Submitted to publisher 19.04.2019, Printed in 11.06.2019, Print format 70x100/16, Printed copies 70.

ISSN 1314-3123 (Print)
ISSN 2534-9457 (Online)

ISSN 2534-9457 (Online)
ISSN 1314-3123 (Print)

ECONOMICS 21

Year IX, Book 1, 2019

- The 10 Don'ts to Manager's Efficiency
- Infrastructure Charges Levied in Air Transportation – Current Issues and Perspectives
- Protection against Fraud in Electronic Trade Payments

INTERUNIVERSITY JOURNAL

Икономика 21
Година IX, книга 1 2019
Year IX, Book 1, 2019
Economics 21

TO THE READERS AND AUTHORS OF ECONOMICS 21

Economics 21 publishes **research studies, articles and methodological papers**.

1. Volume

Studies: min. - 26 pages; max. - 40 pages;
Articles: min. - 12 pages; max. - 25 pages;
Methodological papers - up to 40 pages.

2. Submission of materials

- On paper and electronically (on CD and/or by e-mail).

3. Technical characteristics

- Written in Word 2003 (at least);
- Page size - A4, 29-31 lines / 60-65 characters per line;
- Line spacing - Single;
- Font - Times New Roman 12 pt;
- Margins - Top - 2.54 cm; Bottom - 2.54 cm; Left - 3.17 cm; Right - 3.17 cm;
- Page numbers - bottom right;
- Footnotes - size 10 pt;
- Charts and graphs - Word 2003 or Power Point.

4. Layout

- Name of article, name of author, scientific degree, scientific title - font Times New Roman, 12 pt, capital letters Bold - justified;
- Employer and address of the place of employment; contact telephones and E-mail;
- Abstract in Bulgarian - up to 15 lines; keywords - from 3 to 5;
- **JEL** classification code for research papers in economics (http://ideas.repec.org/j/index.html);
- The main body of the paper;
- Tables, charts and graphs must be embedded in the text (allowing for language correction and translation);
- Formulae must be created with Equation Editor;
- References in alphabetical order – in Cyrillic and Latin script;
- Technical characteristics and layout:

Template: https://www.uni-svishtov.bg/samagazine/upload/Economics-21-Template_bg.doc

5. Citation guidelines

When citing sources authors should observe the requirements of **APA Style** at: http://www.apastyle.org/ or at http://owl.english.purdue.edu/owl/resource/560/01/ or at http://www.calstatela.edu/library/guides/3apa.pdf.

Each author bears responsibility for the ideas presented, the content and layout of his/her text.

6. Contacts

Editor-in-chief: tel.: (++359)631-66-338
Stylistic editor: tel.: (++359)631-66-335
E-mail: i.varbanov@uni-svishtov.bg, economics21@uni-svishtov.bg
Address: D. A. Tsenov Academy of Economics, 2 Em. Chakarov str., Svishtov, Bulgaria