ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(33)

Publisher
http://jssidoi.org/esc/home

ASPECTS OF THE SECURITY USE OF PAYMENT CARD PIN CODE ANALYSED BY THE METHODS OF MULTIDIMENSIONAL STATISTICS*

Antonín Korauš[1], Ján Dobrovič[2], Jozef Polák[3], Stanislav Backa[4]

[1] Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava 35, Slovak Republic
[2,3,4] University of Prešov in Prešov, Faculty of Management, Konštantínova 16, 080 01 Prešov, Slovak Republic

E-mails:[1] antonín.koraus@minv.sk , [2] jan.dobrovic@unipo.sk , [3] jozefpolak64@gmail.com ,[4] stanislav.backa@gmail.com

Received 14 February 2019; accepted 20 April 2019; published 30 June 2019

Abstract. The conception of economic security management should be established on instruments and measures that will enable the financial institutions to operate in their interest without losing their financial stability, profitability and economic independence. This is a significant prerequisite for the security of the functional components of the company's financial security. The article presents an analysis of research results. Its objective is to contribute to the knowledge and understanding of the behaviour of payment card users with a special focus on the aspect of their security connected with the use of payment card personal identification number (PIN). The article analyses the opinions and attitudes of respondents toward the questions dealing with the security of payment cards and their behaviour when using them. The analysis is carried out from the aspect of gender, age and education of respondents by using multidimensional statistical methods, namely factor analysis and analysis of dispersion.

Keywords: economic security; PIN; financial security; security management; financial institution; security; payment cards

Reference to this paper should be made as follows: Korauš, A.; Dobrovič, J.; Polák, J.; Stanislav Backa, S. 2019. Aspects of the security use of payment card pin code analysed by the methods of multidimensional statistics, *Entrepreneurship and Sustainability Issues* 6(4): 2017-2036. http://doi.org/10.9770/jesi.2019.6.4(33)

JEL Classifications: F5, F52, K42, K24

Additional disciplines (besides field of economics reflected in JEL classifications): information and communication; security, protection of people and property

* *The contribution is the result of Vega project no. 1/0194/19 "Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business".*

1. Introduction

Digital security threats and incidents have been intensified in recent years, thus leading to significant economic and social consequences for public and private organizations as well as individuals. Some examples include disruption of operations (e.g. through denial of service or sabotage), direct financial loss, lawsuits, reputational damage, loss of competitiveness (e.g. in case of theft of trade secret), as well as loss of customer trust. An increasing number of stakeholders are aware of the need of improving the management of digital security risk to reap the benefits of the digital economy.

Risk is the effect of uncertainties on objectives. Digital security risk is the expression used to describe a category of risks related to the use, development and management of the digital environment in the course of any activity. This risk can result from the combination of threats and vulnerabilities in the digital environment. They can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or environment. Digital security risk is dynamic in nature. It includes aspects related to the digital and physical environments, people involved in the activity and organisational processes supporting it.

The activities undertaken by companies in pursuance of their objectives are subject to factors that can have consequences on the likelihood of their success. Risk is the effect, or the consequence, of uncertainty on the objectives pursued by stakeholders, i.e., a deviation from their anticipated reality. Risk is often expressed in terms of likelihood and impact, while risk levels are typically represented on an X-Y axis, which helps in considering the various combinations of these two dimensions.

2. Theoretical background

A number of scientists have devoted their works to the management of economic and financial security at the banking level (Jančíková, Pasztorová 2018; Jančíková, Veselovská 2018). Korauš et al. (2019a, 2019b) analyze the security of payment systems. Athanasoulis et al. (1999) seek to establish a link between the state of macro-markets and financial security. Delaquil et al. (2012) combine problems in assessing the level of economic, energy and climate security (Žuľová et al. 2018) and confirm the need for integrated protection of the state security in various areas. Hacker et al. (2014) develop the methodological aspects to assess the level of the country's economic security. The authors suggest using an Economic Security Index while diagnosing the economic security state. They also justify the possibility of its application as a new measurement tool for research and analysis of state policy on the one hand, and as a new means of assessing economic security of American workers and their families, on the other. Klein (2009) establishes the relationship between the level of economic security and human well-being.

Awareness of security risks research Kordik and Kurilovská (2018), reliable risk assessment method RM/RA CRAMM applicable for a crime risk assessment was described by Mamojka and Mullerova (2017) and its legal questions by Mullerova and Mamojka (2017).

Managing the financial security of financial intermediaries has its own characteristics. Cybernetic security issues, which are often perceived as synonymous with the safety of critical infrastructure (Dobrovič et al., 2017). The problems of conceptualizing the management of economic and financial security of banking institutions are raised by European scientists. Namely, Jantoń-Drozdowska and Mikołajewicz-Woźniak (2017); Shive and Forster (2017) specify the peculiarities of a fraud-monitoring organization within the system of economic security management of a banking institution. Baldwin et al. (2011); Mura et al. (2018) offer a methodical approach to the formation of organizational and economic support for the financial security management of banks. Novotný

(2015), Poliačiková (2017), Paulík et al. (2015) and Gaigaliene et al. (2018) studied the application of CSR measuring model in commercial banks in relation to their financial performance.

Banks currently use sophisticated tools to track and detect fraud and fight against them at every stage of the buying process, even before they buy. Banking experts are constantly expanding and enhancing technology to take a step forward from fraudsters, so that once MasterCard identifies smartphone clips as its own, no one else can shop with client mobile credentials. Card payer cardholders are also able to make safer digital payments even through tokenisation - the process of exchanging a token card master account number.

The smart cards are equipped with an additional security element, which is embedded in the form of an inserted microchip, safely storing user data.

The service provider is assigned or the user selects the Personal Identification Number (IPIN) numbers that contain 3 to 6 digits. PIN numbers are typically associated with different types of banking services. If a user completes a transaction, it is a requirement for users to enter their PIN assigned to their account. User numbers will be verified based on saved numbers. Sometimes a dynamically generated number called a one-time password (OTP) can be used as a PIN. Although PINs are simple and effective in securing accounts, they are prone to attacking the shoulder. When attacking the shoulder surf, the attacker follows the user authentication process and identifies the PIN number. Using virtual keyboard shortcuts makes it easier for an attacker to make keyboard entries on the screen. A security precaution to prevent this attack ensures that no one is entered before the PIN is entered. But in public places such as ATMs, cyber cafes, department stores, etc. It's hard to push. Another option is to use OTP for transactions. However, additional costs and delays could arise. OTP attacks are also prevalent (Raddum et al. 2010).

In the case of a human arm attack, the attackers rely on their ability to observe and remember the details they have observed (Tari et al. 2006; Roth and Richter 2006; Por 2013; Malek et al. 2006; Horecký, 2018). When entering a PIN on a virtual keyboard, a user clicks the numbers one at a time and gives enough opportunity for the observer to see individual digits reconstruct the entire PIN. So any security mechanism that prevents direct entry of numbers and increases the trouble of the attacker tracking the pin input to track the real number is enough to alleviate attacks on the shoulder. But when the attack on the shoulder is surfing with a recording device such as a mobile camera or malware that could record video activity on the screen, it is very difficult to defend (Wu 2014). This is because the attacker could view the recorded video several times and reproduce the PIN number in succession. There are many suggestions to limit recorded attacks on the shoulder. Such models are more complicated for implementation and follow-up for regular users.

Recognizing the potential for PIN attacks during the PIN process, many scientists have focused on developing new schemes to mitigate these attacks. A survey of many virtual keyboards takes place in (Kölsch and Turk 2002). Method (Wilfong 1999) requires that the user performs a math operation on each digit of his / her random number PIN provided by the authenticators. The result is entered by the user. At the end of the server, the same digits are repeated to get digits. Verified based on actual saved PINs. This approach requires users a certain level of competence to perform mathematical computations, and may lead to several erroneous inputs.

In the mobile environment, there is a high risk of the observing attacks which is the way to steal a password, because many people have a camera-equipped mobile phone and a miniature camera. The biometric authentication technology is one of the methods to solve this problem. However, some equipment does not have the device of biometric authentication. Moreover, some system requires PIN or password when failing in the biometric authentication. The PIN or password authentication is still used widely (Fujita, Hirakawa, 2008).

3. Material and methods

The present article deals with the results of research and subsequent analysis. It aims to contribute to the knowledge and comprehension of the behaviour of payment card users with a special focus on the aspect of their security. The article analyses the opinions and attitudes of respondents toward the questions dealing with the security of payment systems and their behaviour when using payment cards. The analysis is carried out from the aspect of gender, age and education of respondents by using multidimensional statistical methods, namely factor analysis and analysis of dispersion. The research as well as the selection of representative sample were carried out as follows:

Time horizon of the survey: 20.02.2018 – 20.07.2018
Representative sample: 1,012 respondents
Number of questionnaires issued: 4,700
Number of (completed) questionnaires collected: 3,288

The representative sample containing 1,012 respondents was selected by random number generator from fully completed questionnaires (3,288) in such a way that it would represent the population of Slovakia over 18 years of age from the aspect of their education, size of municipality and region they live in, and occupation.

The analyzed set is represented in five age categories in ranges 18-30 years, 31-40 years, 41-50 years, 51-60 years and over 60 years. These categories are composed of 206, 212, 192, 196 and 213 respondents, respectively, which represents 2.22%, 20.80%, 18.84%, 19.23%, and 20.90% of the analyzed set, respectively. The research was conducted on 540 men (52,99%) and 479 women (47.01%). Geographically, the respondents were from the regions of Prešov, Košice, Banská Bystrica Žilina, Nitra, Trenčín, Trnava and Bratislava in amounts 134 (13.15%), 140 (13.74%), 117 (11.48%), 127 (12.46%), 127 (12.46%), 144 (14.13%), 112 (10.99%) and 118 (11.58%), respectively. The statistical set was composed of respondents with primary (n=300; 29.44%), secondary (n=438; 42.98%) and university education (n=281; 27.58%). The analysed sample is composed of respondents living in towns (n=518; 50.83%) and villages (n=501; 49.17%). The structure of respondents can be seen in Figures 1 – 4.

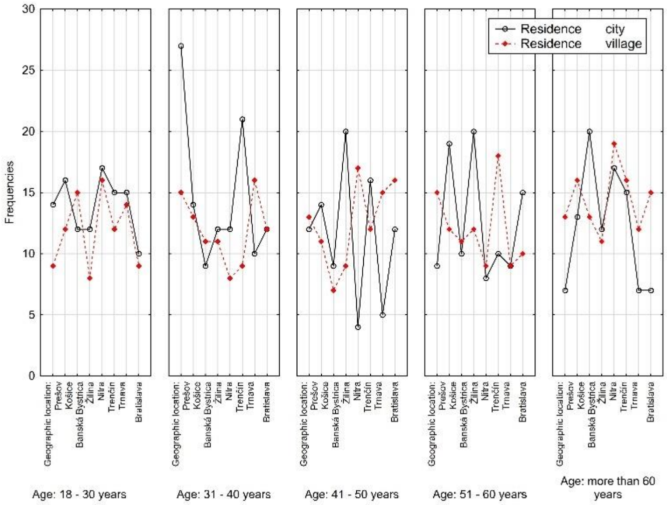

Figure 1. Structure of representative sample per residence, age and geographic region
Source: Own study

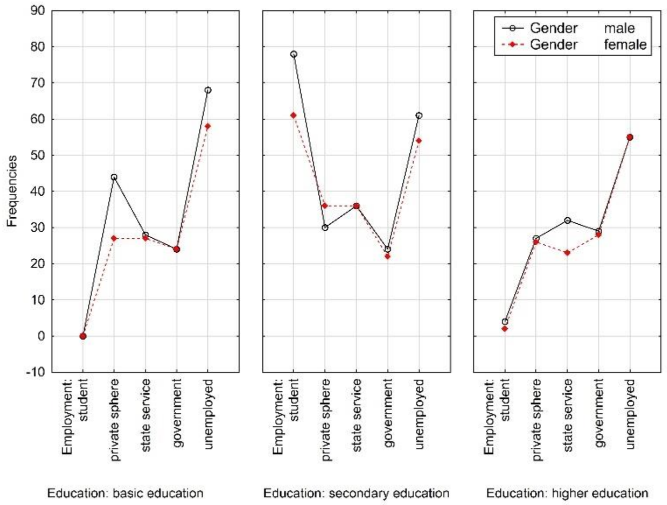

Figure 2. Structure of representative sample per education, gender and employment
Source: Own study

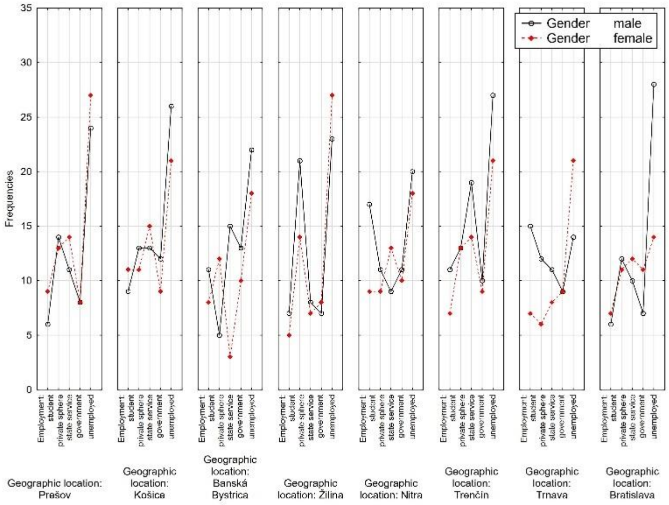

Figure 3. Structure o representative sample per gographich region, gender and employment
Source: Own study

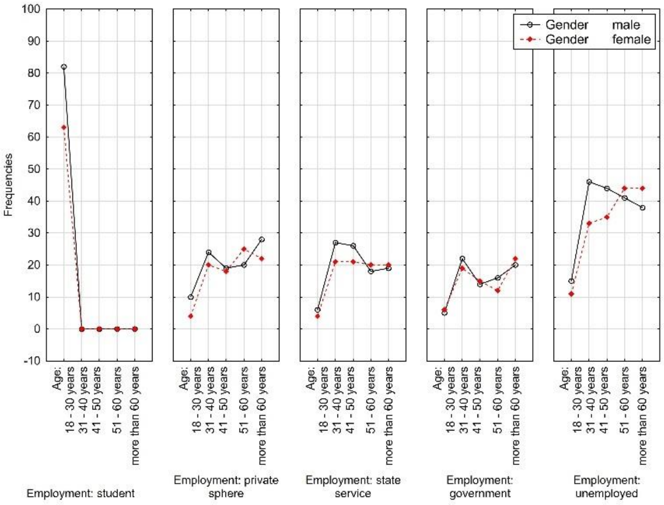

Figure 4. Structure of representative sample per employment, gender and age
Source: Own study

4. Results

The analysis of the behaviour of respondents when making a payment and their opinions on their security was based on answers to questions as follows:

- Q1 – Do you carry your payment card PIN code along with your payment card?
- Q2 – Have you ever changed your payment card PIN code?
- Q3 – Have you altered your payment card PIN code in a way that it would encode your date of birth?
- Q4 – Do you consider ATMs located at banks' premises safer for withdrawing your cash?
- Q5 – Do you have trust in the security of payment systems?
- Q6 – Do personal data represent information that needs to be most importantly protected?
- Q7 – Do you rely on the security measures of your bank in payment cards?
- Q8 – Are you sure that your bank takes proper care of your money?
- Q9 – Do you have any experience with a hacking attack or bank fraud?
- Q10 – Do you think that security measures taken to protect payment card data are continuously getting better?
- Q12 - How confident are you in the security of payment systems?
- Q13 – Do you think that the payment system carries elements of high security risks?
- Q18 – Does the enhanced security of new payment methods outweigh the cost of their implementation?
- Q19 – Does the enhanced customer convenience of new payment methods outweigh the cost of their implementation?
- Q20 - Why is it more challenging to secure payment card information?
- Q22 - How confident are you that customers can protect themselves when their personal information is lost or stolen?

The reliability of the research tool was judged by using the Cronbach's alfa coefficient. Its value was 0.81694. Based on the latter value, it is possible to state that it is not necessary to increase the value by removing any of variables. As the Cronbach alfa exceeds the value of 0.7, we can state that the research tool is reliable, and we can safely process the data.

The method is foremostly aimed at simplifying the description of group with mutual linear dependent signs, i.e. decomposing the source data matrix into structural and noise matrices. Each of main components represents a linear combination of original signs. Main components are ordered in line with their importance, i.e. with the decreasing dispersion (Tab. 1). This implies that a major portion of information on variability of original data is concentrated in the first main component and just as much information is concentrated in the last main component.

Table 1. Table of original values in the source matrix of researched set

Value number	Eigenvalues of correlation matrix, and related statistics			
	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	1,971471	12,32169	1,97147	12,3217
2	1,255233	7,84521	3,22670	20,1669
3	1,202084	7,51302	4,42879	27,6799
4	1,128291	7,05182	5,55708	34,7317
5	1,069369	6,68356	6,62645	41,4153
6	1,054192	6,58870	7,68064	48,0040
7	1,020088	6,37555	8,70073	54,3795
8	0,971202	6,07001	9,67193	60,4496
9	0,932597	5,82873	10,60453	66,2783
10	0,858880	5,36800	11,46341	71,6463
11	0,838353	5,23971	12,30176	76,8860
12	0,827242	5,17026	13,12900	82,0563
13	0,806948	5,04343	13,93595	87,0997
14	0,772271	4,82669	14,70822	91,9264
15	0,706586	4,41616	15,41481	96,3425
16	0,585192	3,65745	16,00000	100,0000

The table of original values in source data matrix (Tab. 1) shows that the concentrations of first, second, third, fourth, fifth, sixths and seventh main components are 12.32169 %, 7.84521 %, 7.51302 %, 7.05182 %, 6.68356 %, 6.5887 %, and 6.37555 % of variability of the original data, respectively. These seven main components, whose own number is larger than 1, concentrate within themselves 54.3795 % of variability of original data of the researched set. The diagram of the dispersion measures (Fig. 5) shows that the first main component divides the responses by vertical axis into two clusters, while at negative values of the component score of the first main component, the responses to 16 of posed questions (Q1 - Q10, Q12, Q13, Q18 – Q20 and Q22) are homogenous. As opposed to the latter, at positive values of component score of the first main component, the responses are more heterogenous. In combinations of second, third, fourth, fifth, sixth and seventh main components, the data are concentrated around the centre of the coordinate system and yield a homogenous structure in all directions.

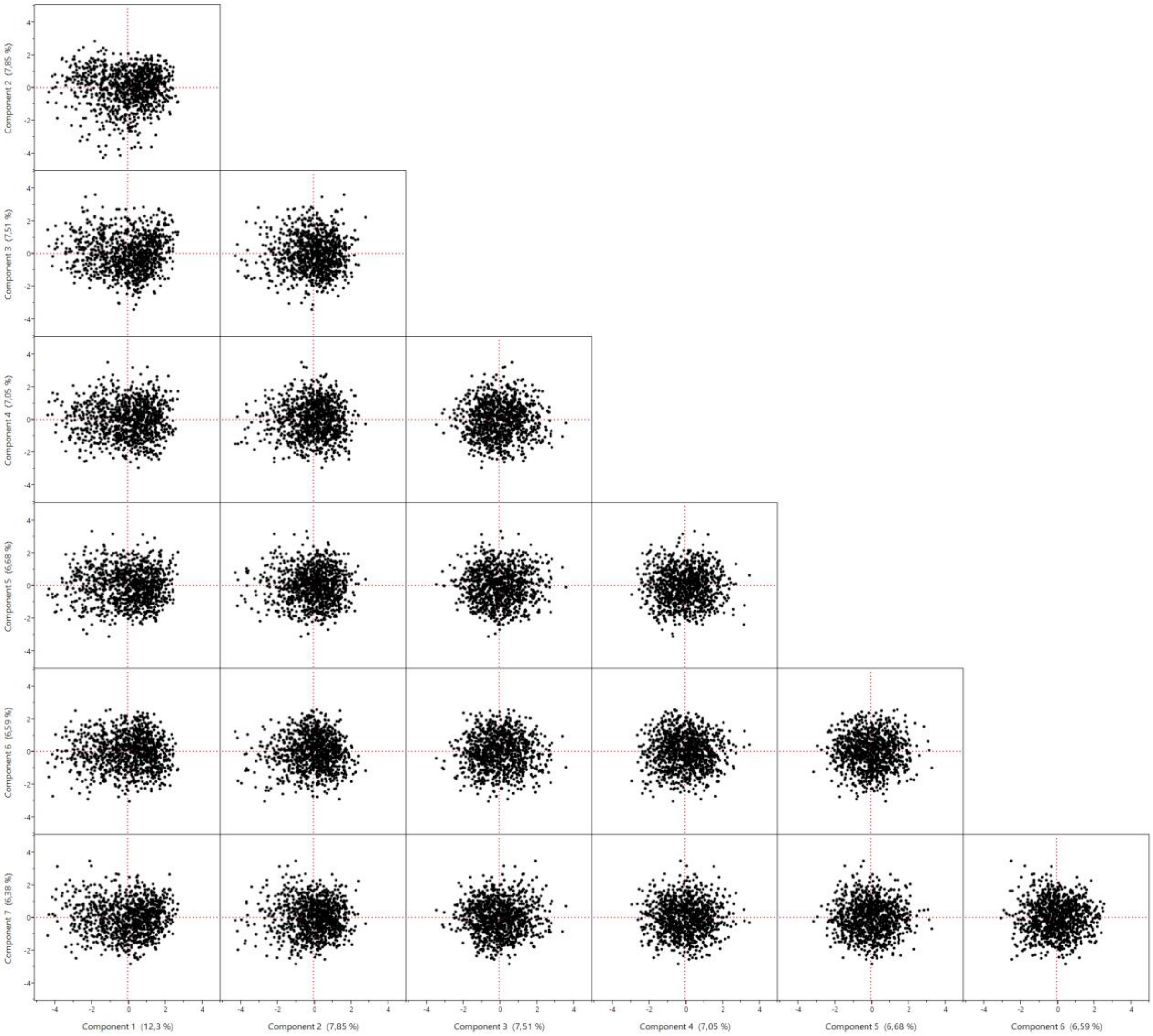

Figure 5. Dispersion diagram of component score
Source: Own study

The appropriate use of factor analysis is tested by Kaiser-Mayer-Olkin (KMO) statistics and Bartlett's test of sphericity. KMO statistics represents an index which serves for comparing the size of experimental correlation coefficients against the size of partial correlation coefficients. When the sum of squares of partial correlation coefficients between all pairs of signs is small in comparison to the sum of squares of pair correlation coefficients, the measure of KMO statistics approaches the value of 1. Low values of KMO statistics indicate that the factor analysis of original signs would not be a good approach because the correlation between the pairs of signs cannot be explained by means of the rest of signs. In accord with the value of Keiser-Mayer-Olkin statistics (0.642) and definition by Kaiser, it is possible to state that based on the used research tool, the measure of correlation is good and the choice of factor analysis for security of payment system is justified. Bartlett's test of sphericity represents a statistical test of correlation between original signs. It tests the null statistic hypothesis H_0 , namely whether "the correlation between the signs does not exist" , i.e. whether the correlation matrix is a unit matrix. The achieved level of significance of Bartlett's test of sphericity p= 0.000 is lower than the level of significance chosen by us (α = 5 %). Thus, we can reject the null hypothesis that the realization of the selected correlation matrix with 16 considered variables is a unit matrix. Hence, to start off, we can state that the factor analysis is appropriate for the data dealing with security of payment system.

Table 2. Assumptions for the use of factor analysis (KMO statistics, Bartlett's test)

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,642
Bartlett's Test of Sphericity	Approx. Chi-Square	629,915
	df	120
	Sig.	0,000

Source: Own study

The first step to the interpretation of results of factor analysis is to analyse the factor matrix (Tab. 3) which serves for gaining the initial number of factors. The factor matrix contains factor loading for each sign, while in each factor, it represents the best linear combination of original signs while including the highest possible number of variability of signs. The first factor is always the most important because it represents the best linear relation found in original signs. The second factor represents the second best linear relation of original data, however it is restricted by a condition that it has to be orthogonal to the first factor. The factor loading explains the role of each original sign in defining the common factor. It is, in fact, a correlation coefficient between every original sign and factor.

Table 3. Factor loading

Variable	**Factor Loading (Varimax normalized) Extraction: Principal components**						
	Factor 1	**Factor 2**	**Factor 3**	**Factor 4**	**Factor 5**	**Factor 6**	**Factor 7**
Q1	0,667027	-0,056201	-0,009635	-0,057215	-0,047914	0,043137	-0,028946
Q2	-0,702289	-0,104631	0,149141	0,124769	-0,036834	0,127380	-0,138716
Q3	0,667834	0,008599	-0,008697	0,068546	0,022302	-0,218077	0,061900
Q4	0,030219	0,678758	-0,245063	0,044069	-0,098954	0,045068	0,133751
Q5	0,019901	-0,140903	0,650951	-0,000812	-0,066915	0,115440	0,296767
Q6	0,049937	-0,040089	0,062699	0,054951	0,009874	0,030645	0,783608
Q7	-0,014691	-0,126738	-0,064008	-0,134143	-0,056402	-0,732862	-0,095482
Q8	0,217457	0,031563	-0,055021	0,084674	0,078457	-0,654224	0,092631
Q9	-0,170928	0,049245	-0,095052	0,580158	0,203906	-0,203738	0,052174
Q10	-0,483641	0,224774	0,010966	-0,129255	-0,019166	-0,117729	0,352577
Q12	-0,202965	0,096779	0,555906	-0,202640	0,115733	0,055215	-0,145093
Q13	-0,062923	0,535860	0,004331	-0,038624	0,076363	0,080119	-0,338568
Q18	-0,031518	0,614785	0,422922	0,040299	0,008766	-0,002696	0,019843
Q19	0,055803	-0,088242	0,361737	0,298743	-0,592838	-0,237350	-0,194491
Q20	0,048449	-0,076490	0,168337	0,176893	0,804773	-0,122083	-0,100801
Q22	0,076839	0,000956	-0,051205	0,730203	-0,096729	0,236042	0,006834
Expl.Var	1,756082	1,254472	1,176141	1,104870	1,097575	1,238837	1,072751
Prp.Totl	0,109755	0,078404	0,073509	0,069054	0,068598	0,077427	0,067047

Source: Own study

The Table 3 makes it obvious that the first factor significantly correlates with components of research tool, namely with Q1 (Do you carry your payment card PIN code along with your payment card?), Q2 (Have you ever changed your payment card PIN code?), and Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth?). The values of factor loading reach the values of 60.7027 % and 66.7834 at components Q1 and Q3, respectively. The positive sign of factor loading reflects the indirect proportion, i.e. the evaluation of responses decreases on Likert scale with an increase in the number of respondents. Thus, in frame of the scale value, the responses stating "certainly not" or "no" are chosen. The factor loading of Q2 component of the research tool reaches the value of -70.2289. As it implies further from the analysis of Table 3, 44.4925 % of variability of Q1 component ("Do you carry your payment card PIN code along with your payment card"), 49,321 % of variability of component Q2 ("Have you ever changed your payment card PIN code?") and 44,6002 % of variability of component Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth?") are explained by the first mutual factor. The second mutual factor correlates with the component Q4 (Do you consider ATMs located at banks' premises safer for withdrawing your cash?"), Q13 ("Do you think that the payment system carries elements of high security risks?") and Q18 ("Does the enhanced security of new payment methods overweigh the cost of their implementation?") with the value of factor loading of 67.8758 % at component Q4, 53.586 % at component Q13, and 61.4785 % at component Q18. This implies that 46.0712 % of variability of component Q4, 28.7146 % of component Q13, and 37.7961% of variability of component Q18 are explained by the second mutual factor. The third mutual factor significantly correlates with the components Q5 ("Do you have trust in the security of payment systems?") and Q12 ("How confident are you in the security of payment systems?") with values of factor loading of 65.0954 % and 55.5906 %. From Table 3, it further implies that the variability values of 42.3737 % and 30.9031 % of Q5 and Q12 components, respectively, are explained by third mutual factor.

The fourth mutual factor correlates with components Q9 ("Do you have any experience with a hacking attack or bank fraud?") and Q22 ("How confident are you that customers can protect themselves when their personal information is lost or stolen?") with values of factor loading of 58.0158 % at Q9 component and 3.0203 % at Q22 component, which represents the values of 33.6583 % and 53.3196 % of variability of these components explained by the fourth mutual factor. The fifth mutual factor correlates with components Q19 ("Does the enhanced customer convenience of new payment methods outweigh the cost of implementation?") and Q20 ("Why is it more challenging to secure payment card information?") with factor loading values of -59.284 % and 80.4773 %, which represent the variability values explained by fifth mutual factor, namely those of 35.1457 % and 64.766 % of Q19 and Q20 components, respectively. The sixth mutual factor correlates with components Q7 ("Do you rely on the security measures of your bank in payment cards?" and Q8 ("Are you sure that your bank takes proper care of your money?"). The factor loading values are -59.284 % and -65.422 % for Q7 and Q8 components of research tool, respectively. Both components yield a negative degree of correlation. The last, seventh extracted factor correlates with Q6 component ("Do personal data represent information that needs to be most importantly protected?") with factor loading value of 78.3608 % which represents a variability of 61.4041 % of this component explained by seventh mutual factor. Aside from defining the basic mutual correlations, we have tested also the practical significance of factors.

Based on the facts mentioned above, the factors of the main research objective, defined as a restriction of main identifiers of the security of payment systems and secure behavior of respondents, can be postulated as follows:

- Factor 1 – PIN code
- Factor 2 – Awareness of security risks,
- Factor 3 – Knowledge of security elements,
- Factor 4 – Personal experience with fraud,
- Factor 5 – Enhancement of security of payment systems,

- Factor 6 – Trust in banks
- Factor 7 – Need of protecting the security elements.

The factor analysis focuses foremostly on parameters of the factor model. It may require estimations of mutual factors, which is referred to as factor score. The values of mutual factors in *n* selected observed objects or observations are not only a useful tool for diagnosing the data, but possibly also an important entry into further analyses. The factor score is not an estimation of parameters in common sense because it involves estimations of values of non-observed quantities. The estimations of factor score for a given object can be imagined as its coordinates in R-dimensional space.

Table 4. Coefficients of factor score

Variable	**Factor Score Coefficients Rotation: Varimax normalized Extraction: Principal components**						
	Factor 1	**Factor 2**	**Factor 3**	**Factor 4**	**Factor 5**	**Factor 6**	**Factor 7**
Q1	0,403974	-0,013833	0,052359	-0,061879	-0,025194	0,116074	-0,046696
Q2	-0,398755	-0,128143	0,058275	0,125695	-0,041488	0,025549	-0,119585
Q3	0,375695	0,057193	0,070984	0,054799	0,030542	-0,108248	0,042342
Q4	0,027875	0,548057	-0,210160	0,038413	-0,103424	0,005812	0,141195
Q5	0,072687	-0,104559	0,553875	0,010329	-0,027592	0,069398	0,255593
Q6	0,015465	-0,015685	0,039837	0,040412	0,018702	0,018291	0,727772
Q7	-0,102795	-0,061977	-0,027040	-0,115261	-0,078224	-0,606415	-0,076729
Q8	0,050911	0,078406	0,009138	0,079014	0,053975	-0,524822	0,092201
Q9	-0,137283	0,047838	-0,066609	0,528113	0,171820	-0,190067	0,054055
Q10	-0,301059	0,168865	-0,042920	-0,110880	-0,033603	-0,173483	0,350339
Q12	-0,045912	0,066089	0,467854	-0,163334	0,123199	-0,001508	-0,140003
Q13	0,011815	0,417752	0,011906	-0,024544	0,064394	0,035366	-0,305297
Q18	0,054389	0,502483	0,376989	0,055539	0,018987	-0,064813	0,019703
Q19	0,023964	-0,043568	0,321691	0,283831	-0,534320	-0,225482	-0,197507
Q20	0,049374	-0,056303	0,197145	0,166662	0,740724	-0,074662	-0,096994
Q22	0,055867	-0,000993	-0,032630	0,656919	-0,080331	0,198365	-0,007713

Source: Own study

In line with the defined goals of research, the subsequent section deals with the analysis of respondents' opinions or attitudes represented by factor score in relation to extracted identifiers, factors of payment system security by means of Fisher's ANOVA. Within the analysis, we shall be considering only the impact of significant independent variables or that of their interactions on the value of respective factor at the selected level of significance α = 0.05.

ANOVA is an acronym standing for analysis of variance. ANOVA serves for comparing various sources or characteristics of various classes. These sources are referred to as factors and can contain several various levels. The goal is to decide whether the mean value of the measured quantity differs for various factors. This is demonstrated by testing the hypothesis on the impact of factor on the mean value. In this case, the zero hypothesis states that the mean values of tested groups do not differ significantly.

Table 5. ANOVA for Factor 1 (Payment card PIN code)

Effect	Univariate Tests of Significance for Factor n.1 Sigma-restricted parameterization Effective hypothesis decomposition				
	SS	Degr. of Freedom	MS	F	p
Intercept	0,0739	1	0,07385	0,10685	0,743829
Age	70,5132	4	17,62831	25,50408	0,000000
Gender	0,0455	1	0,04549	0,06581	0,797591
Education	130,3322	2	65,16608	94,28025	0,000000
Age*Gender	2,6284	4	0,65709	0,95066	0,433863
Age*Education	28,9456	8	3,61820	5,23470	0,000002
Gender*Education	0,7795	2	0,38977	0,56391	0,569160
Age*Gender*Education	4,6 555	8	0,58194	0,84193	0,565697
Error	683,5923	989	0,69120		

Source: Own study

The Table 5 shows that a change in Factor 1 (Payment card PIN code) expressed by factor score is significantly influenced by the age of respondents, their education, and mutual interaction of age and education, namely at the level of significance of α = 5 %. When the factor score is, as a result of factor analysis, considered a measure of consent, attitude or importance for the respondent, while a positive or negative number represents a positive perception and importance or negative attitude and unimportance of the given factor for respondents, respectively, then we can state that the average value of factor score for the category of 18 – 30 years of age represents a value of -0.651576.

This can be interpreted as unimportance of the given factor for the observed age category of respondents.
The category of 31-40 years of age reaches the factor score of –0.062128. Hence, also for the latter age category, this factor is unimportant while achieving a lower value when expressed in absolute terms.

The age category of 41-50 years achieves the average value of -0.10293 of factor score, which indicates an indifferent attitude of respondents to the problem of using payment card PIN code. A change in value, and therefore increase in importance represented by positive values of average factor score can be found in categories of 51-60 and over 60 years of age, where it achieves values of +0.38045 and +0.350828, respectively. The average values of factor score for individual age categories for the extracted factor referred to as payment card PIN code are graphically depicted in Figure 6.

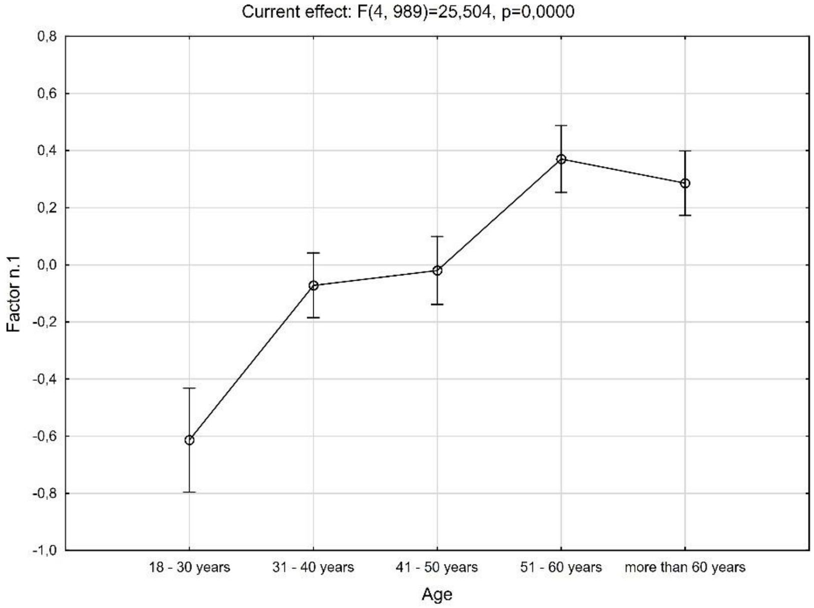

Figure 6. Dependence of average value of factor score on age category of respondents
Source: Own study

The second factor significantly influencing the value of achieved factor score for the first extracted factor is that relating to education of respondents. This implies from Table 5 based on the achieved levels of significance (p=0.000000). The average value of achieved factor score for respondents with primary education is 0.338203, which indicates a positive perception of the problem of payment card PIN code as a security feature and its importance for the latter category of respondents. Equally positive values of factor score are also those achieved for the group of respondents with secondary education, in whom, however, the average value is 0.117786. The negative values of factor score for respondents with university education achieve the average of -0.544667. The average values of factor score for individual education categories for the second extracted factor (referred to as Payment card PIN code) are graphically depicted in Figure 7.

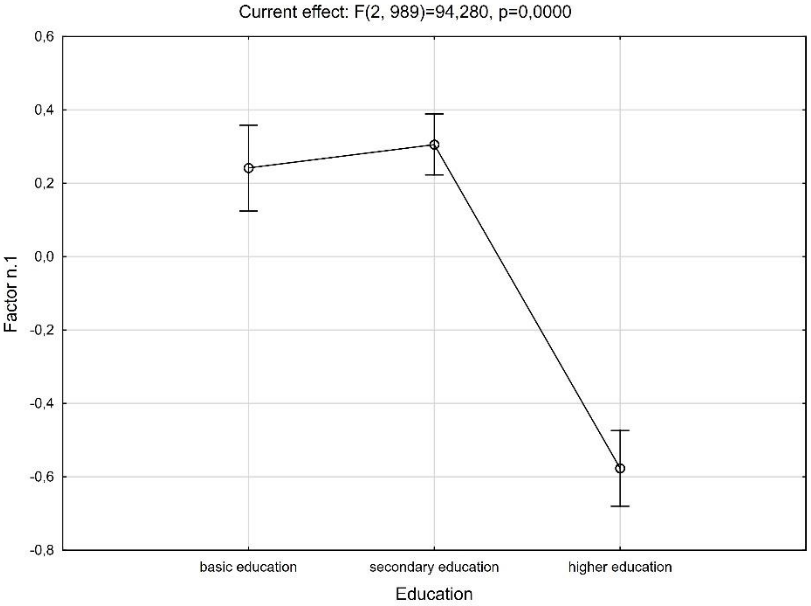

Figure 7. Dependence of average value of factor score for Factor 1 on education of respondents
Source: Own study

The Table 5 further shows that based on the level of significance (p=0.000002), the average value of achieved factor score for the first extracted factor referred to as Payment card PIN code is significantly influenced also by the interaction of age and education of respondents. This is illustrated in Figure 8.

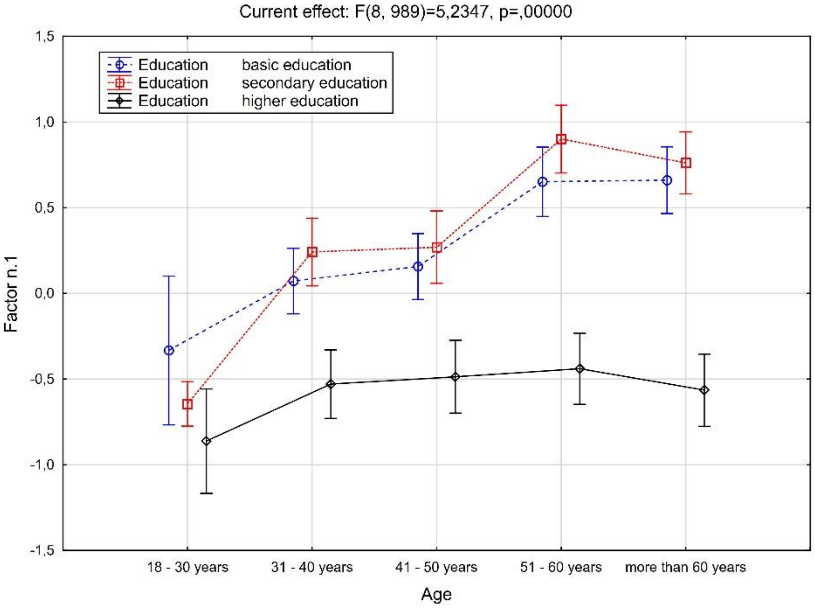

Figure 8. Dependence of average value of factor score for Factor 1 on the interaction of age and education of respondents
Source: Own study

The Figure 8 shows that the increase in age in respondents with primary education brings about also an increase in the average value of factor score, however the increase in age in categories over 51 years of age ceases to be reflected in the average value. A similar trend in average value of factor score can be seen also in respondents with secondary education, although the category older than 60 years of age yields a decrease. The basic statistical characteristics of values of factor score for the interaction of age and education are given in Table 6.

Table 6. Statistical characteristic of the achieved factor score for Factor 1 and interaction of age and education of respondents

Effect	**Level of Factor**	**Level of Factor**	**N**	**Factor n.1 Mean**	**Factor n.1 Std.Dev.**	**Factor n.1 Std.Err**	**Factor n.1 -95,00%**	**Factor n.1 +95,00%**
Total			1019	0,000000	1,000000	0,031327	-0,06147	0,061472
Age*Education	18 - 30 years	basic education	17	-0,336385	0,938893	0,227715	-0,81912	0,146349
Age*Education	18 - 30 years	secondary education	160	-0,646981	0,527793	0,041726	-0,72939	-0,564573
Age*Education	18 - 30 years	higher education	29	-0,861699	0,337073	0,062593	-0,98991	-0,733483
Age*Education	31 - 40 years	basic education	75	0,089651	0,891998	0,102999	-0,11558	0,294881
Age*Education	31 - 40 years	secondary education	68	0,241486	1,054671	0,127898	-0,01380	0,496771
Age*Education	31 - 40 years	higher education	69	-0,526318	0,468148	0,056358	-0,63878	-0,413856
Age*Education	41 - 50 years	basic education	72	0,159906	0,953586	0,112381	-0,06418	0,383988
Age*Education	41 - 50 years	secondary education	60	0,262373	1,093952	0,141229	-0,02023	0,544970
Age*Education	41 - 50 years	higher education	60	-0,487197	0,586230	0,075682	-0,63864	-0,335758
Age*Education	51 - 60 years	basic education	65	0,649781	0,904951	0,112245	0,42555	0,874017
Age*Education	51 - 60 years	secondary education	68	0,894503	1,111443	0,134782	0,62548	1,163529
Age*Education	51 - 60 years	higher education	63	-0,451054	0,483099	0,060865	-0,57272	-0,329387
Age*Education	more than 60 years	basic education	71	0,657839	0,999955	0,118673	0,42115	0,894525
Age*Education	more than 60 years	secondary education	82	0,757533	1,066848	0,117814	0,52312	0,991946
Age*Education	more than 60 years	higher education	60	-0,568299	0,498832	0,064399	-0,69716	-0,439437

Source: Own study

The initial results presented in Table 5 do not sufficiently answer the basic question as to which age and education groups of respondents differ from each other in relation to the value of achieved factor score. A more profound understanding of the differences between individual significant factors influencing the change in average value of factor score for the first extracted factor can be aided with the use of Scheffe's test.

Table 7. The result of Scheffe's test per age category and value of factor score for Factor 1

Cell No.	**Scheffe test; variable Factor n.1 Probabilities for Post Hoc Tests Error: Between MS = ,69120, df = 989,00**					
	Age	**{1} -,6516**	**{2} -,0621**	**{3} -,0103**	**{4} ,38084**	**{5} ,35083**
1	18 - 30 years		0,000000	0,000000	0,000000	0,000000
2	31 - 40 years	0,000000		0,983129	0,000010	0,000033
3	41 - 50 years	0,000000	0,983129		0,000281	0,000826
4	51 - 60 years	0,000000	0,000010	0,000281		0,997879
5	more than 60 years	0,000000	0,000033	0,000826	0,997879	

Source: Own study

Table 7 shows that for the level of significance of α=5 %, there exists a significant difference in the average value of the achieved factor score between age category 18-30 years of age and all other observed age categories, between age categories 31-40 and 51-60 years of age and between those of 31-40 and over 60 years of age. Then we can find a significant difference in the average value of factor score between age categories 41-50 and 51-60 years of age and at the same time also in relation to the category over 60 years of age. On the other hand, statistically insignificant differences can be found between age categories 31-40 and 41-50 years of age and those over 60 and 61-60 years of age.

Table 8. The result of Scheffe's test per education category and value of factor score for Factor 1

Cell No.	Scheffe test; variable Factor n.1 Probabilities for Post Hoc Tests Error: Between MS = ,69120, df = 989,00			
	Education	**{1} ,33820**	**{2} ,11779**	**{3} -,5447**
1	basic education		0,001993	0,00
2	secondary education	0,001993		0,00
3	higher education	0,000000	0,000000	

Source: Own study

The results of Scheffe's test (Tab. 8) indicate that there is a significant mutual difference between the average value of achieved factor score between individual groups of education of respondents.

The present analysis clearly shows that the attitude of respondents to the problem of basic rules of using the payment card PIN code (Q1: Do you carry your payment card PIN code along with your payment card?; Q2: Have you ever changed your payment card PIN code?; Q3: Have you altered your payment card PIN code in a way that it would encode your date of birth?) is influenced foremostly by age, education and mutual interaction of age and education of respondents. The analyzed data have shown that 94.17 % of respondents at 18-30 years of age definitely do not carry the payment card PIN code along with their payment card, while in category over 60 years of age, the percentage is 64.32 %. On the other hand, the payment card PIN code is carried along with the payment card only in 5.8 % of respondents at 18-30 years of age, while in the category over 60 years of age, the total percentage is 33.8 %. As to this first question, there is a similar finding also from the aspect of education of respondents. While in category of respondents with primary education, the payment card PIN is carried along with the payment card in 30.3 %, in those with secondary education, the percentage is 26.7 %, and in those with university education, the percentage is as low as 5.3. As to the second question of the research tool (Q2: Have you ever changed your payment card PIN code?), we are coming to similar conclusions as in the precedent component. As many as 93.20 % of respondents in category of 18-30 years of age have changed their payment card PIN code, while in the same category on the other side of Likert's scale, the proportion is 4.9 %. On the other hand, a certain positive feature in conceiving the basic security rules can be found also in the category over 60 years of age, which is considered to be a risk category from the aspect of security of payment systems. In the latter category, as many as 65.73 % of respondents have changed their payment card PIN code. Nevertheless, as many as 30.00 % of respondents of the latter age category have not changed their payment card PIN code. The second question was answered positively and thus the payment card PIN code was changed by 70.3 %, 71.9 % and 93.6 % of respondents with primary, secondary and university education, respectively. The last component of the first extracted factor, namely Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth?) represents most possibly the weakest point in payment card users who are often unaware of the risk it poses to them. As few as 4.4 % of respondents at 19-30 years of age have a date of birth encoded in their PIN code, while in the category over 60 years, their proportion is 38.50 %. The present analysis leads to a conclusion that the level of information on risks associated with the use of payment card PIN code is insufficient especially in older people and those with primary information. Naturally, a more profound analysis of further extracted factors would be needed to arrive at comprehensive understanding of the habits exposing the users of payment cards to risks associated with using the PIN code. Unfortunately, the scope of the present analysis is not that wide. However, the authors intend to analyse further factors with the use of multidimensional statistical methods.

Conclusions

The present analysis clearly shows that the attitude of respondents to the problem of basic rules of using the payment card PIN code (Q1: Do you carry your payment card PIN code along with your payment card?; Q2: Have you ever changed your payment card PIN code?; Q3: Have you altered your payment card PIN code in a way that it would encode your date of birth?) is influenced foremostly by age, education and mutual interaction of age and education of respondents. The analyzed data have shown that 94.17 % of respondents at 18-30 years of age definitely do not carry the payment card PIN code along with their payment card, while in category over 60 years of age, the percentage is 64.32 %. On the other hand, the payment card PIN code is carried along with the payment card only in 5.8 % of respondents at 18-30 years of age, while in the category over 60 years of age, the total percentage is 33.8 %. As to this first question, there is a similar finding also from the aspect of education of respondents. While in category of respondents with primary education, the payment card PIN is carried along with the payment card in 30.3 %, in those with secondary education, the percentage is 26.7 %, and in those with university education, the percentage is as low as 5.3. As to the second question of the research tool (Q2: Have you ever changed your payment card PIN code?), we are coming to similar conclusions as in the precedent component. As many as 93.20 % of respondents in category of 18-30 years of age have changed their payment card PIN code, while in the same category on the other side of Likert's scale, the proportion is 4.9 %. On the other hand, a certain positive feature in conceiving the basic security rules can be found also in the category over 60 years of age, which is considered to be a risk category from the aspect of security of payment systems. In the latter category, as many as 65.73 % of respondents have changed their payment card PIN code. Nevertheless, as many as 30.00 % of respondents of the latter age category have not changed their payment card PIN code. The second question was answered positively and thus the payment card PIN code was changed by 70.3 %, 71.9 % and 93.6 % of respondents with primary, secondary and university education, respectively. The last component of the first extracted factor, namely Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth?) represents most possibly the weakest point in payment card users who are often unaware of the risk it poses to them. As few as 4.4 % of respondents at 19-30 years of age have a date of birth encoded in their PIN code, while in the category over 60 years, their proportion is 38.50 %. The present analysis leads to a conclusion that the level of information on risks associated with the use of payment card PIN code is insufficient especially in older people and those with primary information. Naturally, a more profound analysis of further extracted factors would be needed to arrive at comprehensive understanding of the habits exposing the users of payment cards to risks associated with using the PIN code. Unfortunately, the scope of the present analysis is not that wide. However, the authors intend to analyse further factors with the use of multidimensional statistical methods.

There are different parts of the payment process that need to be secure. Firstly, the account access needs to be limited to authorized users only. Traditionally, authorized users can be identified by government-issued identification, passwords, signatures, and other information about a person such as her favorite sports team, name of her first-grade teacher, or that of the first street that she lived on. To some extent, such information can be accessed by unauthorized users. Biometrics can be also the means of authenticating. While biometrics has long been part of science fiction and spy movies, only recently, consumers are able to use their fingerprints to access sensitive data and approve payments. While still in the early stages of adoption, fingerprint authentication is likely to expand in the coming years. Secondly, the exchange of live account credentials that are used to make purchases is extremely high. Payment card numbers along with demand deposit numbers are commonly asked for to make purchases. Once these numbers are in the possession of unauthorized users, the likelihood of fraud increases. Thirdly, fraud associated with making payments when accounts do not have sufficient funds can be eliminated by buyers instructing their financial institutions to make payment. Given today's technology and online connectivity, payment instruments such as checks where real-time account and sufficient balance verification are not generally available should be eliminated for large purchases or transfers. Some countries have had great success in eliminating checks. Fourthly, payment providers often take on additional liability to encourage usage which may have the unintended effect of reducing incentives for cardholders to make prudent decisions regarding keeping live payment credentials secure. However, significant fraud continues to occur and these costs may be reduced if consumers were held accountable for not adequately safekeeping their payment credentials (Chakravorti, S. 2016).

Acknowledgement

The contribution is the result of Vega project no. 1/0194/19 "Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business".

References

Athanasoulis, S., Shiller, R., & Van Wincoop, E. (1999). Macro Markets and Financial Security. *FRBNY Economic policy review*, *5*(1), 21-39. Retrieved from https://www.newyorkfed.org/ medialibrary/media/research/ epr/99v05n1/9904atha.pdf

Baldwin, A., Beres, Y., Duggan, G. B., Mont, M. C., Johnson, H., Middup, C., & Shiu, S. (2011). *Economic Methods and Decision Making by Security Professionals*. Retrieved from https://researchportal.bath.ac.uk/en/publications/ economic-methods-and-decision-making-by-security-professionals

Bányász, P. (2018) The emergence of cyber security in the scientific community, Military Engineer (XIII) II1 362 XIII year 3, number - Conference: Tudomány kapujában September 2018, https://doi.org/10.13140/RG.2.2.28913.33124

Delaquil, P., Goldstein, G., Nelson, H., Peterson, T., Roe, S., Rose, A., Wei, D., & Wennberg, J. (2012). *Developing and Assessing Economic, Energy, and Climate Security and Investment Options for the US.* (2012 International Energy Workshop Paper). Center for Climate Strategies. Retrieved from https://www.decisionwaregroup. com/assets/ccs_strategic-investment-project_report.pdf

Dobrovič, J., Gombár, M., & Benková, E. (2017). Sustainable development activities aimed at combating tax evasion in Slovakia. *Journal of Security and Sustainability Issues*, 6(4): 761-772. https://doi.org/10.9770/jssi.2017.6.4(19)

Gaigaliene, A., Jurakovaite, O., & Legenzova, R. (2018). Assessment of EU banking network regionalization during post-crisis period. *Oeconomia Copernicana*, 9(4) : 655-675. https://doi.org/10.24136/oc.2018.032

Hacker, J. S., Huber, G. A., Nichols, A., Rehm, P., Schlesinger, M., Valletta, R., & Craig, S. (2014). The Economic Security Index: A New Measure for Research and Policy Analysis. *Special Issue: Economic Insecurity: Challenges, Issues and Findings*, *60*(S1), 5-32. https://doi.org/10.1111/roiw.12053

Horecký, J. (2018). Operation and action of a trade union (in terms of Czech Republic labour law). *Central European Journal of Labour Law and Personnel Management*, 1(1) : 17 – 27 . http://doi.org/10.33382/cejllpm.2018.01.02

Chakravorti, S. (2016) New Payment Technologies: Back to Basicsin Digital Transformation of Payment Media conference organized by Funcas, May 26, 2016 in Madrid, Spain. http://doi.org/10.2139/ssrn.2781264

Jančíková, E., & Veselovská, S. 2018. The new Technologies and the Fight Against Money Laundering and the Terrorism Financing. In *2nd International Scientific Conference - EMAN 2018 - Economics and Management: How to Cope With Disrupted Times*, Ljubljana - Slovenia, March 22, 2018, ISBN 978-86-80194-11-0. https://doi.org/10.31410/EMAN.2018.334

Jančíková, E., & Pásztorová, J. (2018). Strengthened EU Rules to Tackle Money Laundering and Terrorism Financing and their Implementation in Slovak Republic. In Staníčková, M., L. Melecký, E. Kovářová and K. Dvoroková (eds.). *Proceedings of the 4 th International Conference on European Integration 2018* . Ostrava: VŠB - Technical University of Ostrava, 2018, pp. 528-536. ISBN 978-80-248-4169-4. ISSN 2571-029X.

Jantoń-Drozdowska, E., & Mikołajewicz-Woźniak, A. (2017). The impact of the distributed ledger technology on the Single Euro Payments Area development. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, 12(3) : 519–535. https://doi.org/10.24136/eq.v12i3.28

Korauš, A., Gombár, M., Kelemen, P., Backa, S. 2019a. Using quantitative methods to identify security and unusual business operations. *Entrepreneurship and Sustainability Issues,* 6(3): 1101-1012. http://doi.org/10.9770/jesi.2019.6.3(3)

Korauš, A., Dobrovič, J., Polák, J., Kelemen, P. 2019b. Security position and detection of unusual business operations from science and research perspective. *Entrepreneurship and Sustainability Issues,* 6(3):1270-1279. http://doi.org/10.9770/jesi.2019.6.3(15)

Kordík, M., Kurilovská, L., Intra Group Compliance Agreement as a tool to manage the risks in the daughter companies. *Enterpreneurship and Sustainability Issues*, 5(4):1008-1019, https://doi.org/10.9770/jesi.2018.5.4(21)

Klein, J. (2009). The Politics of Economic Security: Employee Benefits and the Privatization of New Deal Liberalism. *The Journal of Policy History*, 16(1): 34-65. https://doi.org/10.1353/jph.2004.0002

Mamojka, M.; & Müllerová, J. (2016). New methodology for crisis management RM/RA CRAMM and its legal frame. In: Production management and engineering sciences. - Leiden: CRC Press/Balkema, 2016. pp 185-190. ISBN 978-1-138-02856-2.

Mura, L., Marchevska, M., & Dubravska, M. (2018). Slovak Retail Business Across Panel Regression Model. *Marketing and Management of Innovations*, 4, pp. 203-211. http://doi.org/10.21272/mmi.2018.4-18

Müllerová, J., & Mamojka, M. 2017. Legal possibilities of the rescue forces during the emergency event. In: SGEM2017 Conference Proceedings, 29 June-5 July, 17(51): 605-612. ISBN 978-619-7408-08-9/ISSN 1314-2704. https://doi.org/10.5593/sgem2017/51/S20.079

Novotný, J. (2015). Customer segmentation and customer relationship management. *Acta Oeconomica Universitatis Selye*, 4 (1) : 114 – 119. ISSN 1338-6581

Paulík, J., Sobeková Majková, M., Tykva, T., & Červinka, M. (2015). Application of the CSR Measuring Model in Commercial Bank in Relation to their Financial Performance. *Economics and Sociology*, 8(4): 65-81. http:// dx.doi.org/10.14254/2071- 789X.2015/8-4/5

Poliačiková, E. (2017). Perception of types of markets of customers in Slovakia. Acta Oeconomica Universitatis Selye 6 (1) : 129 – 136. ISSN 1338-6581

Shive, S. A., & Forster, M. M. (2017). The Revolving Door for Financial Regulators. *Review of Finance, 21*(4), 1445-1484. https:// doi.org/10.1093/rof/rfw035

Žuľová, J., Švec, M., & Madleňák, A. (2018). Personality aspects of the employee and their exploration from the GDPR perspective. *Central European Journal of Labour Law and Personnel Management*, 1(1), 68 – 77. http://doi.org/10.33382/cejllpm.2018.01.05

Acknowledgements

The contribution is the result of Vega project no. 1/0194/19 "Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business".

Short biographical note about the contributors at the end of the article (name, surname, academic title and scientific degree, duties, research interests):

Assoc. Prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA is an associate professor at Academy of the Police Force in Bratislava, Slovak Republic. Research interests: economy security, finance security, cyber security, energy security, finance, banking, management, AML, economic frauds, financial frauds, marketing, sustainability.
ORCID ID: https://orcid.org/0000-0003-2384-9106

Assoc. Prof. Ing. Ján DOBROVIČ, PhD, is an associate professor in the Department of Management, Faculty of Management at the University of Prešov in Prešov since 2006. Since 2013, he works as head of the Department of Management, and he teaches school subjects: management, operations management, and logistics. From 1996 to 2001 he was appointed Regional Director of the Slovak Trade Inspection in the Prešov Region Prešov. Between 2001 - 2005 he became the municipal office in Prešov. Between 2006 - 2010 he held the position of Deputy for International Relations, Director General of the Slovak Tax Directorate. He is also involved in public offices as a member of the city council and deputy Prešov Self-Governing Region.
ORCID ID: https://orcid.org/0000-0002-0637-106X

Ing. Jozef POLÁK, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0003-4733-0851

JUDr. Stanislav BACKA, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0002-0411-4158