University of Salford A Greater Manchester University
University of Essex ESSEX BUSINESS SCHOOL International Centre for Entrepreneurship Research
The General Jonas Žemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
Vilnius Gediminas Technical University
RISEBA
Estonian Business School
NATO Energy Security Centre of Excellence
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2017 June Volume 6 Number 4
http://doi.org/10.9770/jssi.2017.6.4(3)

THE SAFETY RISKS RELATED TO BANK CARDS AND CYBER ATTACKS

Anton Korauš[1], Ján Dobrovič[2], Rastislav Rajnoha[3], Ivan Brezina[4]

[1,4]Paneuropean University in Bratislava, Faculty of Economics and Entrepreneurship, Tematinská 10, 851 05 Bratislava, Slovak Republic

[2]University of Prešov in Prešov, Faculty of Management, Konštantínova 16, 080 01 Prešov, Slovak Republic

[3]Tomas Bata University in Zlín, Faculty of Management and Economics, Mostní 5139, 760 01 Zlín, Czech Republic

E-mails: [1]antonin.koraus@paneurouni.com; [2]jan.dobrovic@unipo.sk; [3]rajnoha@fame.utb.cz; [4]brezina.ivan@yahoo.com

Received 20 November 2016; accepted 27 February 2017

Abstract. In accordance with the rise and rapid growth in e-commerce in thepastfewdecades, the use of payment cards for online purchases has significantly increased in the payment cards market. This situation has led to an explosion in payment card fraud and it is costing billions of euros and dollars in losses in the card payment industry. The understanding of security has thereforeundergone a significantdevelopment. Due to the inaccurate evaluation of their personal security status, people tend to underestimate the safety features related to the protection of their financial data on the internet. This claim is supported by the high level of interest that cyber attackers show in persons operating in the public and economic spheres. The collection and data analysis carried out suggests that the target sample group has not had experience with cyber-attacks, predominantly because this group was made up of 'ordinary' people, presumably outside of the cyber attackers' sphere of interest. It is therefore important to further investigate the opinion and consumer approach to security and payment card fraud. As a result of rising losses, financial institutions and card issuers are constantly searching for new technologies and innovations in payment card fraud detection and prevention. This article provides several views on personal safety and quality of security to payment cars and cyber- attacks.The data collection and analysis was carried out in Slovakia via electronic sample surveys. With sample surveys the data is collected from a base sample unit, which in this case consisted of a sample of residents of the Slovak Republic. The research sample for this investigation consisted of 287 respondents, out of which there were 164 men (57,14%) and 123 women (42,86%). For the purposes of the analysis, the respondents were divided into categories, based on their age, level of education and occupation. The study results can help the issuers of payment cards and banks as well as clients using payment cards, especially in order to improve the prevention against fraud and the unauthorised use of payment cards.

Key words: cyber-attacks, security, safety risk, customer, bank payment cards, payment card fraud, card payment industry

Reference to this paper should be made as follows: Korauš, A., Dobrovič, J., Rajnoha, R., Brezina, I. 2017. The safety risks related to bank cards and cyber attacks, *Journal of Security and Sustainability Issues*, 6(4): 563-574. http://doi.org/10.9770/jssi.2017.6.4(3)

JEL Classifications: D18, F 52, G21, K 24

1. Introduction

Despite the payment card industry's significant improvement in reducing the rate of fraud, absolute losses from payment card fraud continue to grow. All participants involved in the payment system are affected. In addition to the direct financial losses incurred from fraud, there are growing concerns that increased public attention to data breaches and payment card fraud may lead to a general undermining of consumer confidence in electronic payments.

Importantly, the very nature of fraud risk is changing (Jankalová, Jankal, R. 2017; Štitilis et al. 2016; Allabouche et al. 206; Tumalavičius et al 2017; Lavrinenko et al. 2016; Lavrinenko et al.2017; Kabát et al. 2017; Sulphey, Alkahtani 2017). As consumers have become more comfortable using many payment options across a growing range of channels, the landscape has become more complex, leading to new vulnerabilities and risks for fraud. The perpetrators of payment fraud have changed as well. Today, professional, well-funded criminal groups, operating domestically and internationally, are using the latest technologies to attack global and regional payment networks (Čirjevskis 2016; Apsītis et al. 2016; Tumalavičius et al. 2016; Teletov et al. 2017; Teivāns-Treinovskis, Amosova 2016; Baronienė, Žirgutis 2017; Limba et al. 2017).

The banking area receives strategically timely information about fraudulent activities. Many of the banks and very large databases contain valuable business information that can be extracted from these data stores (Ogwueleka 2008; Munteanu, Tamošiūnienė 2015; Kaźmierczyk, Aptacy 2016; Jurevičienė, Skvarciany 2016;). Valid payment card fraud detection in two classes (real) process of identifying those transactions that are fraudulent and fraudulent transactions (Maes et al. 2002). Bhatla et al. (2003) argues that the payment card fraud can generally be classified into three categories:

- traditional card fraud (stolen cards, card application, acquisition, imitation and fake accounts),
- business related fraud (dealer collusion and triangulation)
- internet related fraud (site cloning, generating credit cards and false merchant sites).

The transaction with payment cards may take place within minutes, but the side effects of fraud over phone lines orvia electronic communication is able to continue for months, sometimes years in the form of long and costly legal proceedings. When electronic fraud strikes, the losses are usually distinguished, while the client's reaction ranges from strong anger to distrust toward the bank which "has allowed" the fraud to happen. Trustworthiness is the essential determinant of efficient and stable banking.

Nowadays, the secure development has become a real and urgent matter in many countries around the world (Štitilis, Klišauskas 2015; Kriviņš 2015). Regulations and card network operating rules regarding payment card fraud place a substantial burden on the card-issuing community. Therefore, card issuers are highly motivated to identify areas of vulnerability in the system and to champion tools for preventing fraud. Issuers also have to balance the management of fraud risk with its POS impact on their cardholders.

Personal economic and financial security can be mostly viewed as a matter of personal decision and common sense (Kalyugina at al. 2015). Currently, it is the phenomenon of globalization and diversification, which is becoming dominant, and that to such extent that the majority of economic subjects take action in accordance with what is called "rational inattention" (see Sims 2006). At the same time, personal debt and economic freedom have become the key elements of every society (Rakauskienė 2014; Šileika, Bekerytė 2013; Mura, Sleziak 2015; Rajnoha et al. 2016 a; Rajnoha et al. 2016c).

Security is connected to a large number of bank activities and is a significant issue in commercial bank management. Ensuring the security of banking is determined by a range of factors. Commercial bank security is a complex system including many activities, e.g. capital management in the context of credit, market and operational risks (i.e. capital adequacy management), etc. The security process is focused on operational risk defined as a risk of loss resulting from internal processes or human capital failure or from external conditions (Peker et al. 2014).

Physical security is connected to the protection of cash in bank branches and ATMs. The system security includes all internal and external processes carried out by informational system. In this context, the security of individual customers´ deposits and their payments is crucial. The security of customers´ is the key factor of success for banks. The mentioned factor heavily influences acquisition, retention or loss of customers. For that reason, it is decisive for a commercial bank to undertake such measures to ensure a proper and efficient protection of customers (Korauš et al. 2016).

The present situation demands the commercial banks to pay extraordinary attention to payment cards security. The compliance with consumers' needs and requirements (Bilan, 2013), bank customers' satisfaction and comprehensive customer care are nowadays at the centre of attention for researchers and bankers. It is for this reason that these respective factors represent an important marketing instrument for many companies, notably those working at highly competitive markets. (Belás and Demjan, 2014) Researchers are trying to find the main determinants for bank customer satisfaction and examine these issues from various perspectives (Doležal et al., 2015; Belás et al., 2015; Chochoľáková et al., 2015; Paulík et al., 2015; Štilinis et al 2015; Štilinis et al 2016).

A key to the success of the modern payment card industry has been its ability to gain and then maintain consumer confidence in the safety and security of these payment systems. Networks, issuers, acquirers, and regulators have all played their respective roles in effectively managing payment fraud, thus greatly contributing to the rapid growth in consumer adoption of electronic payments. Nevertheless, the nature and scope of payment fraud in these environments is dynamic, and as such it require the ongoing development of new solutions, as well as greater collaboration across all links in the payments chain. Responsible managers will consider how changes in business models, behaviours, and fraud threats are creating new challenges in mitigating the related risks.

2. Theoretical Background

Credit card fraud continues to be a significant and dynamic risk to financial institutions as a result of both new threats and the increasing regulatory interest in fraud management programs. Emerging fraud threats and solutions required to mitigate them are increasingly technically complex. To secure and maintain customers' trust, the financial institutions must prevent, detect and respond to fraud risk in an agile manner through fraud management technologies and predictive analytics. While the new US mandate of Europay, MasterCard and Visa (chip and PIN) technology will help decrease the risk of counterfeit transactions, financial institutions must remain vigilant, as fraudsters will certainly be crafting new modes of attack (Korauš et al. 2016).

The expansion of payment cards has significantly changed the manner we shop and businessmen sell goods and services. Currently, payment cards are vital in most advanced economies. Amromin and Chakravorti (2009) suggest that extensive usage of debit cards has caused lower demand for small-denomination banknotes and coins. This process was seen in thirteen advanced economies. Payment surveys done recently also indicate that consumers are using payment cards instead of checks.

Extensiveusage and acceptance of payment cards leads to a growing number of consumers and at the same time merchants start to prefer payment cards to cash and checks.

In general, all payment tools possess special aspects such as cost, transaction speed, restraint, security, convenience, records keeping and acceptance (Hajduová, et al. 2014; Schuh and Stavins, 2011; Ching and Hayashi, 2006; Borzekowski et al., 2006; Ključnikov, et al. 2016; Virglerová, et al. 2016).

Schuh and Stavins (2011) define payment security as "security against permanent financial loss or wanted disclosure of personal information when a payment method has been stolen, misused, or accessed without the owner's permission". According to the research by Zinman (2008), the improved security was a significant proximate of recent growth of debit card users. The customers tend to choose transactions which are secure because in their eyes the payment security is of crucial importance.

A lot of cardholders prefer holding bank cards as a preventative measure against loss, robbery, theft, or counterfeit money. As opposed to the latter approach, there are others who are still fond of using cash instead of cards, as they are afraid of becoming exposed to the risks of fraudulent activities when the cards are lost or stolen. Most of the clients feel secure because they are always protected by liability agreements with card issuers and merchants when these problems occur. The concern of security was highlighted in the research by Schuh and

Stavins (2011) who presented their conclusion that people who consider the card payment method relatively more secure are more likely to adopt it and vice versa. Security is definitely important and necessary when it comes to understanding the consumer behaviour for using payment bank cards.

Since the internet environment is more sensitive to system attacks, the utilisation of these channels has underlined the essential role of bank security (Koskosas, 2011; Dhillon and Torkzadeh, 2006). Koskosas (2011) claimsthat customers can find huge advantage in electronic banking due to its simplicity and reduction of transaction costs, however it is necessary to respect the financial security.

The use of electronic banking is tightly associated with the customers´ perception of their security which has an impact on their behaviour and attitudes (Grabner-Krauter and Faullant, 2008). The recognised absence of security is defined as a potential loss caused by fraud or internet banking hacking (Lee, 2009) In this context, the security and privacy are considered to be two fundamental determinants of customer trust in electronic banking (Flavián and Guinalíu, 2006).

Security attributes of electronic banking and payment cards were examined by Hoffmann and Birnbrich (2012). Belás et al. (2016) argue "their research was focused on describing the conceptual and empirical relations among bank activities in the field of protection against third party attacks, customer relationship management quality and customer loyalty". The authors declare that security is crucial and is becoming even more important in the current banking sector. The fraud prevention has become one of the priorities of banks, customers and even politicians as bank frauds harm both banks and customers. The results showed that there is a positive relation between trustworthiness of a bank, its skills in the field of fraud prevention and customer relationship management quality. After all, customer relationship management quality has a positive influence on customer loyalty. There is a difference between younger and older customers in their knowledge about security measures of banks focused on fraud prevention. At the same time, the positive impact of this awareness on the customer relations quality is less significant in the group of older clients. "The possible cause reason for this could be found in a higher level of scepticism of older clients regarding the efficiency of the above-mentioned measures. Fraud prevention is vital in customer relationship management quality for all customers regardless of their education and income levels" (Korauš et al. 2016).

3. Research objective, methodology and data

The basis for the research lies in the discussion of cyber fraud and stems from two Hypotheses.

Hypothesis 1: A significantly larger number of university-educated women compared to men under the age of 40 has no experience with hacking or bank fraud.

Hypothesis 2: A significantly larger number of high-school-educated men compared to women over the age of 40 has no experience with hacking or bank fraud.

Both hypotheses were confirmed.

Introduction:

- Blissful ignorance:
  - The psychological aspect of blissful ignorance- people do not perceive the threats of hacking based on their feeling of false security.
  - Due to the incorrect evaluation of their security, people underestimate safety guidelines connected to financial data protection on the internet.
- Safety features and the updating of security software's
- The hackers' point of view:
  - The feeling of false security most likely comes from the narrow focus of cyber crime on corporations or persons with a high public profile.

- The examples and reasons behind cyber-attacks on corporations, state institutions and banks.
- Results from target group data
- Conclusions:
  - It is clear from the data collection and analysis that the research group did not encounter cyber-attacks mainly due to the fact that it consisted of 'ordinary' people, presumably outside of the zone of interest of the hackers. This claim is supported by the fact that the hackers are predominantly interested in persons operating in the public economic life.

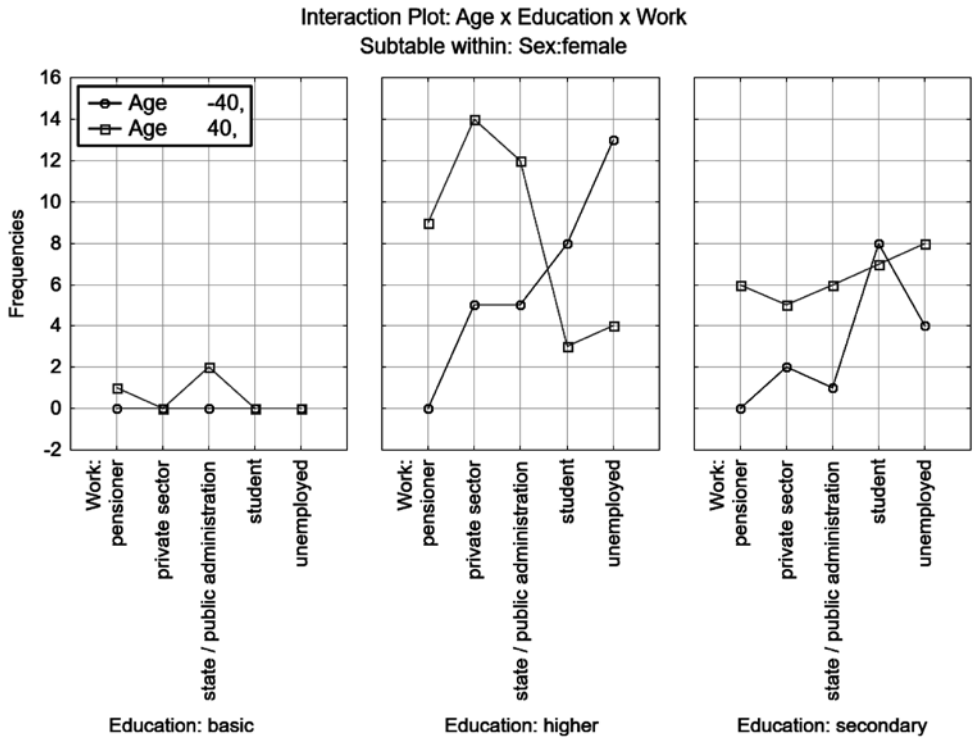
Data Collection

Data collection was conducted in Slovakia through an electronic questionnaire. The survey collected data from a specific part of the base sample group, consisting of the citizens of the Slovak republic. Data collected via surveys do not provide for a reliable data set for all markers, as these are not equally represented with the examined units. However, from a temporal perspective, surveys are very efficient, which can be seen as their greatest advantage. Surveys also facilitate the work with data collection and the processing of data which leads to an efficient use of financial costs. This kind of data collection allows for greater thoroughness of investigation as the smaller the target sample, the bigger the possibility of increasing the investigated content. The sample can be observed more intensively, whereby the amount of information obtained can be greater in volume and examined in greater detail. Surveys can also be used with the destructive character of an exhaustive statistical investigation, ie in cases when the examined unit is devalued by statistical investigation.

The target sample for this experiment consisted of 287 respondents, out of which 164 were men (57,14%) and 123 were women (42,86%). For the purposes of the investigation the respondents were stratified into separate categories by age, education and occupation. The age category saw the respondents separated into two groups, those over and under the age of 40. In the under 40 group there were 113 units (39,37%) and in the over 40 group contained 174 units (68,63%). The education category saw the statistical units divided into three groups. 152 respondents were university educated (52,64%), 120 were high-school educated (41,81%) and 15 reached basic, primary school education (5,22%). Such division roughly corresponds with the education demographic of the populace of the Slovak republic.From an occupational perspective, the respondents were divided into: students (64 - 22,30%), unemployed (64 - 22,30%), employed in state and public sectors (59 - 20,56%), employed in the private sector (64 - 22,30%) and retired (36 - 12,54%).

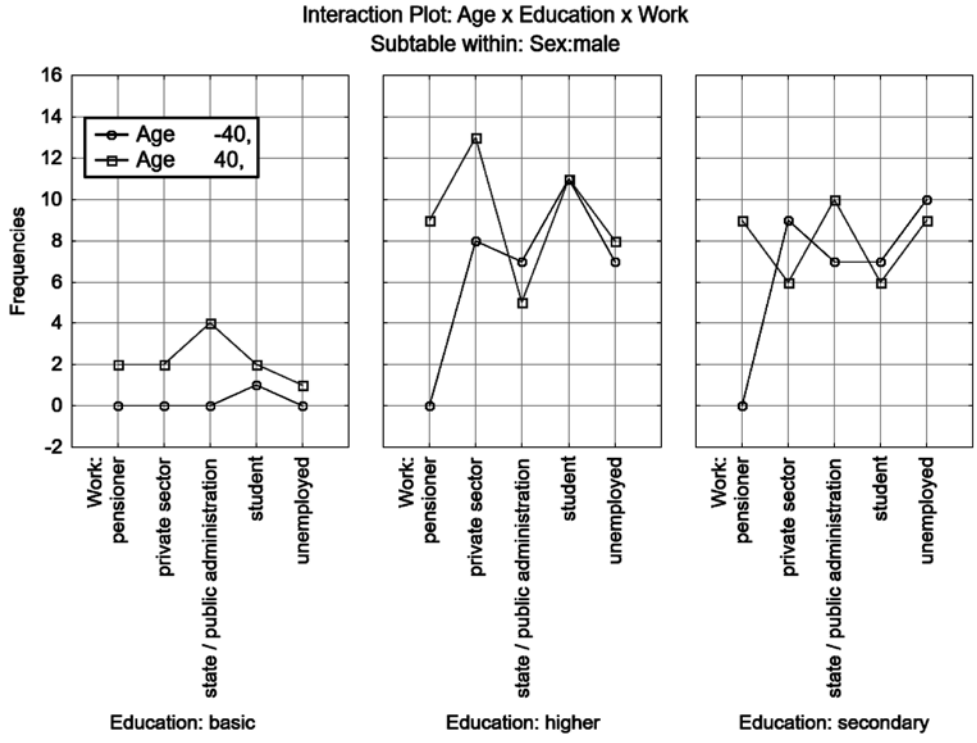
Graph 1, Graph 2: A graphic representation of the respondents in their respective categories, according to gender.

Graph 1: Interaction in the 'women' subset:



Source: collected data

Graph 2: Interaction in the 'men' subset:



Source: collected data

For the purposes of the research on the awareness of people about hacking attacks, a contingency table was created, collating the collected data. Table 1 collates the responses to the question: *Do you have any experience with hacking attacks or bank fraud?*

Table1: A contingency table of responses in the observed categories

Sex	Age	Education	no	yes	**Row Totals**
Male	-40	Higher	23	10	**33**
Male	-40	Secondary	16	17	**33**
Male	-40	Basic	0	1	**1**
Total			39	28	**67**
Male	40	Higher	21	25	**46**
Male	40	Secondary	10	30	**40**
Male	40	Basic	6	5	**11**
Total			37	60	**97**
Female	-40	Higher	14	17	**31**
Female	-40	Secondary	6	9	**15**
Female	-40	Basic	0	0	**0**
Total			20	26	**46**
Female	40	Higher	21	21	**42**
Female	40	Secondary	17	15	**32**
Female	40	Basic	0	3	**3**
Total			38	39	**77**
Columns Total			**134**	**153**	**287**

Source: collected data

Using the contingency table not only allows for the analysis of individual responses, but also creates an idea of the feeling of safety as an umbrella concept, based on personal experience of respondents with hacking attacks. The contingency table also serves as a source of entry data for the Pearson chi-square test, in order to confirm or disprove the hypotheses, which are devised to discern the differences between the feelings of safety of individual genders.

Methodology

Pearson's chi-squared test was used to investigate the target group's data. This test appears feasible for the confirmation or the disproval of the stipulated hypotheses. The Pearson chi-squared test is a fundamental, most frequently-used test of independence in contingency tables. This statistical test tests the null hypothesis, which states that there exists no difference between the expected and theoretical distribution. The arbitrary units X and Y are therefore statistically independent. The probability that a certain variable of the unit X occurs does not in any way affect that a certain variable of the unit Y occurs as well. This fact is expressed through probability, ie through the hypothesis of independence and it stipulates that:

$$p_{ij} = P\left(X = i \wedge Y = j\right) = P\left(X = i\right)P\left(y = j\right) = p_i p_j, \;\; i = 1,\ldots,r; \;\; j = 1,\ldots,c \quad (1)$$

Based on the results of the chi-square test we do not reject the null hypothesis, as long as the differences between the experimental and the expected values occurred as a result of a coincidence and, conversely, we reject the null hypothesis and accept the alternate hypothesis if the differences between expected values are statistically significant. If we mark the number of subjects where a certain observed situation occurred n_{ij} while the value of X equals the value of i, and the value of Y equals the value of j, we can then define the marginal frequency belonging to the i variable of X, or the $j$variable of Y:

$$n_i = \sum_{j-1}^{c} n_{ij} \quad (2)$$

$$n_j = \sum_{i-1}^{r} n_{ij} \tag{3}$$

If we do not reject the null hypothesis we can expect the frequency of individual combinations, when $X=i$ and $Y=j$ which we mark by e_{ij} that we can calculate as the following:

$$e_{ij} = np_{ij} = np_i p_j = \frac{n_i n_j}{n} \tag{4}$$

Pearson confirmed that:

$$X^2 = \sum_{i=1}^{r}\sum_{j=1}^{c} \frac{\left(n_{ij} - e_{ij}\right)^2}{e_{ij}} \tag{5}$$

Once the null hypothesis of independence applies, it has a chi-squared division of probability with the parameters of $(r-1)(c-1)$; therefore $X^2 \sim X^2(r-1)(c-1)$ applies. The null hypothesis of the independence of X and Y is disproved due to the significance ofα, once the value of the tested statistic X^2 exceeds the 100 $(1-\alpha)\%$ quantile of the division of X^2, ie when:

$$X^2 \geq X^2(r-1)(c-1)^{(1-\alpha)}. \tag{6}$$

The assumptions of the Pearson chi-square test that must be verified before the test are the following:

- The individual observations in the contingency table are independent from each other, therefore each unit of the research process is included in the contingency table cell only once.
- At least 80% of the contingency table has an expected multiplicity of (e_{ij}) greater than 5 and all cells of the table have an expected frequency of (e_{ij}) greater than 2. This is tied to the asymptotic features of the X^2 statistic and is therefore as important an assumption as, for example, the assumption of the normal distribution of the observed values in the t-test group.

The results gained by observing the target group

It is clear from the contingency Table 1 that the majority of the respondents have encountered hacking attacks. This is confirmed by the fact that increasingly even persons supposedly outside of the hacker‘s zone of interest are attacked, rather than just persons of a high public and social profile in the country. It is also clear from contingency Table 1 that a certain part of the populace has not yet encountered hacking attacks, which could potentially lead to a false sense of security with the given respondents.

Another factor that was investigated was the focus of the hacking attacks on the respective gender of persons. In order to find out whether there is a difference between the number of hacking attacks on men and women, the following hypotheses were devised:
***Hypothesis 1*:** A significantly larger number of university-educated women compared to men under the age of 40 has no experience with hacking or bank fraud.
***Hypothesis 2*:** A significantly larger number of high-school-educated men compared to women over the age of 40 has no experience with hacking or bank fraud.

The given hypotheses were verified using the Pearson chi-squared test with significance level α = 0.05. The entry data used was obtained from the contingency Table 1, gained by a survey via elecrtronic questionnaire in the Slovak Republic.

Based on the chi-square test conducted using the data from Table 1 (χ2 – 3,945357, p = 0.04700), with α = 0.05,

a significant difference between the answers of university-educated men and women under the age of 40 was shown. We can therefore state that a significantly higher number of university-educated women compared to men under the age of 40 has no experience with hacking or bank fraud.

The same manner of testing was applied to the high-school-educated group. Based on the Perason chi-square test ($\chi 2 - 6{,}000000$, $p = 0.01431$) conducted using the data from Table 1 with $\alpha = 0.05$, we can equally accept Hypothesis 2. The findings indicate that similarly, a significantly larger number of high-school-educated men compared to women over the age of 40 has no experience with hacking attacks or bank fraud.

Conclusions

Criminal activity associated with abusing the banking payment cards is variable. It is determined mostly by technical opportunity for advancement of offenders, inattention from the side of payment card holders and technological progress of society. Financial losses caused by misusing the banking payment cards are very high world-wide (Rajnoha, et al. 2016 b). For that reason, all preventative technical and organisational measures focused against this form of criminal acts are important.

Compared to any other time in its history, the payment card industry faces a rapidly increasing variety of security challenges as the transaction environment grows in size and complexity.

On a global level, fraud continues to migrate from more secure to less secure regions and channels. This obvious shift is accelerated by an increasingly adept and organized criminal community that seeks to exploit security vulnerabilities and commit fraud. Criminals are targeting not only the weakly monitored, stand-alone, point-of-interaction devices, but are also launching sophisticated attacks on the private networks of well-known entities: - such as major data processors and top-tier merchants. All of these factors can lead to fraud attacks.

Credit card fraud has been committed since credit cards were first introduced. Modern technology has increased the ways in which it can be committed. Criminals see the card industry as a lucrative business that can be exploited by the use of technology.

Credit card frauds cantake several forms, ranging from petty theft, where the perpetrators tend to use the credit card for smaller purchases, to greater and more sophisticated attacks, where the goal of the criminal is to alter the safety features of the bank card itself (Snyman 1995). Such cyber frauds are classified as an intentional, illegal attempt at causing an alteration and a distortion of the bank card details.

Consumers perceive that identity fraud is rising, even though research shows it is tapering off. Meanwhile, consumer losses are growing, due to causes ranging from lost or stolen cards and data breaches to theft via online channels, phone, and mail. Issuers must be able to juggle a number of responses, among them education, block-and-reissue, authentication, detection, and provision of various services.

To counter the problem, credit card companies constantly review security features and measures that are applied to cards and devote considerable resources to the maintenance of security systems and programming.

There are numerous challenges to dealing with credit card fraud, particularly since transactions do not require the physical presence of the seller and the purchaser. Since, one of the biggest concerns relating to security in e-commerce applications is the use of the credit/debit cards; the failure to secure the card information can cause a major damage to the organization in terms of financial fraud, identity theft, legal regulations, loss of consumer confidence, etc.

It is therefore important that a new approach, for example an intelligence led approach, be considered in combating card fraud.

Our own research has shown that in case of both hypotheses, i.e. whether the respondents have experience with cy-

ber attacks or banking fraud. From our research it is evident that the majority of respondents has encountered cyber attacks. This is confirmed by the fact that persons of presumably smaller interest than those operating in public and economic spheres are increasingly becoming the objects of cyber attacks. The aspects of payment card protection against counterfeit and unauthorised use begins with card issuers. The production of payment cards requires safety conditions identical to those of banknote printing. It is, however, extremely important to adhere to safety guidelines when carrying and using a bank card. Adherence to such guidelines by the clients, as outlined by all bank card issuers and commercial banks, is the primary pre-requisite for the decrease of the cyber attack success rate.

Based on the analyzed data it is clear that there are people who have not yet personally experienced hacking. Even though they constitute a minority with regards to the research, these people can be the basis for a group that can become the future focus of hackers precisely due to their ignorance of the problem. By informing this group about the existing preventative measures against hacking attacks, the threat of them being attacked can be eliminated. From the hackers‘ point of view and based on the conducted tests, men seem to be a more interesting group to target. The reason for this phenomenon can potentially be that the hackers perceive men to be more likely to hold positions of significance and therefore the data obtained may hold greater value.

Acknowledgment

The contribution is the result of VEGA Project No. 1/0255/2016 The research on the possibility of optimization of process-oriented models of the financial administration management with a focus on transfer pricing and tax harmonization in the terms of EU.”.

References

Allabouche, K.; Diouri, O.; Gaga, A.; El Amrani El Idrissi, N. 2016. Mobile phones’ social impacts on sustainable human development: case studies, Morocco and Italy, *Entrepreneurship and Sustainability Issues* 4(1): 64-73. http://dx.doi.org/10.9770/jesi.2016.4.1(6)

Amromin, G., Chakravorti, S. 2009. „Whither Loose Change?” The Diminishing Demand for Small Denomination Currency, *Journal of Money Credit and Banking* 41 (23): 315335, 2009WP200811.

Apsītis, A.; Joksts, J.; Antanavičienė, J. 2016. Threats to sustainable development: asset grabbing phenomenon and the legal concept of Force and Fear in Roman Law, *Journal of Security and Sustainability Issues* 6(2): 289-297. http://dx.doi.org/10.9770/jssi.2016.6.2(8)

Baronienė, L.; Žirgutis, V. 2017. Cybersecurity facets: counterfactual impact evaluation of measure “Procesas LT” in enterprises of the it sector, *Journal of Security and Sustainability Issues* 6(3): -. http://dx.doi.org/10.9770/jssi.2017.6.3(10)

Belás, J., Korauš, M.; Kombo, F., Korauš, A. 2016. Electronic banking security and customer satisfaction and in commercial banks, *Journal of Security and Sustainability Issues* 5(3): 411-422. http://dx.doi.org/10.9770/jssi.2016.5.3(9)

Belás, J.; Chocholáková, A.; Gabčová, L. 2015. Satisfaction and loyalty of banking customers: a gender approach, *Economics and Sociology* 8(1): 176–188. http://dx.doi.org/10.14254/2071- 789X.2015/8-1/14

Belás, J.; Demjan, V. 2014. Bank customers satisfaction: case studies from Czech Republic, *Actual problems of economics* 12(162): 315–323.

Bhatla T.P.; Prabhu, V.; Dua, A. 2003. Understandingcreditcardfrauds. Cards Business Review# 2003-1, Tata ConsultancyServices.

Bilan, Y. 2013. Sustainable development of a company: Building of new level relationship with the consumers of XXI. Century, *Amfiteatru Economic* 15: 687–701.

Borzekowski, R., Kiser, E. K., Ahmed, S. 2006 „Consumers’ Use of Debit Cards: Patterns, Perferences, and Price Response.” Finance and Economics Discussion Series, p. 10.

Ching, A., Hayashi, F. 2006. „Payment Card Rewards Programs and Consumer Payment Choice.” Payments System Research, Federal Reserve Bank of Kansas City, Issue 0602, pp. 135.

Chocholáková, A.; Gabčová, L.; Belás, J.; Sipko, J. 2015. Bank Customers’ Satisfaction, Customers’ Loyalty and Additional Purchases of Banking Products and Services. A Case Study from the Czech Republic, *Economics and Sociology* 8(3): 82–94. DOI: 10.14254/2071-789X.2015/8-3/6

Čirjevskis, A. 2016. Sustainability in information and communication technologies' industry: innovative ambidexterity and dynamic capabilities perspectives, *Journal of Security and Sustainability Issues* 6(2): 211-226. http://dx.doi.org/10.9770/jssi.2016.6.2(2)

Dhillon, G.; Torkzadeh, G. 2006. Values-focused assessment of information system security in Organizations, *Information Systems Journal,* 16 (3); 293–314.

Doležal, J.; Šnajdr, J.; Belás, J.; Vincúrová, Z. 2015. Model of the loan process in the context of unrealized income and loss prevention, *Journal of International Studies* 8 (1): 91– 106. http://dx.doi.org/10.14254/2071-8330.2015/8-1/8

Flavián, C.; Guinaliu, M. 2006. Consumer trust, perceived security, and privacy policy: three basic elements of loyalty to a web site, *Industrial Management & Data Systems* 106 (5/6): 601–620.

Grabner-Krauter, S.; Faullant, R. 2008. Consumer acceptance of internet banking: the influence of internet trust. *International Journal of Bank Marketing* 26 (7): 483–504. http://dx.doi.org/10.1108/02652320810913855

Hajduová, Z., Andrejkovič, M., Mura, L. 2014. Utilizing experiments designed results during error identification and improvement of business processes. In: Acta PolytechnicaHungarica, Vol. 11, No. 2, 2014, pp. 149-166 ISSN 1785-8860

Hoffmann, A. O. I.; Birnbrich, C. 2012. The impact of fraud prevention on bank-customer relationship, *International Journal of Bank Marketing* 30(5): 390–407. http://dx.doi.org/10.1108/02652321211247435

Jankalová, M.; Jankal, R. 2017. The assessment of corporate social responsibility: approaches analysis, *Entrepreneurship and Sustainability Issues* 4(4): 441-459. http://doi.org/10.9770/jesi.2017.4.4(4)

Jurevičienė, D.; Skvarciany, V. 2016. Camels+t approach for banks' assessment: evidence from the Baltics, *Entrepreneurship and Sustainability Issues* 4(2): 159-173. http://dx.doi.org/10.9770/jesi.2016.4.2(4)

Kabát, L.; Filip, S.; Filipová, L. 2017. Safety measurement peculiarities in selected countries, *Journal of Security and Sustainability Issues* 6(3): 343-356. http://dx.doi.org/10.9770/jssi.2017.6.3(2)

Kalyugina, S.; Strielkowski, W.; Ushvitsky, L.; Astachova, E. 2015. Sustainable and secure development: facet of personal financial issues, *Journal of Security and Sustainability Issues* 5(2): 297–304. DOI: http://dx.doi.org/10.9770/jssi.2015.5.2(14)

Kaspersky Lab 2014. *The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide.*Avalable from: http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

Kaźmierczyk, J.; Aptacy, M. 2016. The management by objectives in banks: the Polish case, *Entrepreneurship and Sustainability Issues* 4(2): 146-158. http://dx.doi.org/10.9770/jesi.2016.4.2(3)

Ključnikov, A., Belás, J., Smrčka, L. 2016. The Role Of Risk-Taking And Competitive Aggressiveness In Management of SMEs, *Polish Journal of Management Studies* 14 (1). ISSN 2081-7452 http://dx.doi.org/10.17512/pjms.2016.14.1

Korauš, A., Dobrovič, J., Ključnikov, A., Gombár, M. 2016. Customer Approach to Bank Payment Card Security and Fraud, *Journal of Security and Sustainability Issues* 6(1): 85–102. http://dx.doi.org/10.9770/jssi.2016.6.1(6)

Koskosas, I. 2011. E-banking security: A communication perspective in Risk management. *Palgrave Macmillan*, Vol. 13, pp. 81–99.

Kriviņš, A. 2015. Towards security and safety: police efficiency across European countries. *Journal of Security and Sustainability Issues* 5(1): 35–44. DOI: http://dx.doi.org/10.9770/jssi.2015.5.1(3)

Lavrinenko, O.; Jefimovs, N.; Teivāns-Treinovskis, J. 2017. Issues in the area of secure development: trust as an innovative system's economic growth factor of border regions (Latvia-Lithuania-Belarus), *Journal of Security and Sustainability Issues* 6(3): 435-444. http://dx.doi.org/10.9770/jssi.2017.6.3(9)

Lavrinenko, O.; Ohotina, A.; Tumalavičius, V.; Pidlisna, O. V. 2016. Assessment of partnership development in cross-border regions' innovation systems (Latvia-Lithuania-Belarus), *Journal of Security and Sustainability Issues* 6(1): 155-166. http://dx.doi.org/10.9770/jssi.2016.6.1(12)

Lee, M. 2009. Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit, *Electronic Commerce Research and Applications* 8 (3):130–141.

Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability Issues* 4(4): 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Maes, S.; Tuyls, K.; Vanschoenwinkel, B.; Manderick, B. 2002. Credit carddetectionusingBayesian and neuralnetworks. Proceeding International NAISO Congress on neuronfuzzy Technologies.

Munteanu, C.; Tamošiūnienė, R. 2015. Modern approaches in quantifying economic security. Case study of Estonia, Latvia, Lithuania and Republic of Moldova, *Journal of Security and Sustainability Issues* 4(4): 596-610. http://dx.doi.org/10.9770/jssi.2015.4.4(2)S

Mura, L., Sleziak, J. 2015. Innovation and Entrepreneurship Network. CERS 2014: 5th Central European Conference in Regional Science, International Conference Proceedings, pp. 643-651. ISBN 978-80- 553-2015- 1

Ogwueleka, F. N. 2008. Credit cardfrauddetectionusingdataminingtechniques. Ph.D. Dissertation. Department of ComputerScience. NnamdiAzikiweUniversity, AwkaNigeria.

Pauceanu, A. M. 2016. Innovation and entrepreneurship in Sultanate of 0man – an empirical study, *Entrepreneurship and Sustainability Issues* 4(1): 83-99. http://dx.doi.org/10.9770/jesi.2016.4.1(8)

Paulík, J.; Kombo, F.; Ključnikov, A. 2015. CSR as a driver of satisfaction and loyalty in commercial banks in the Czech Republic, *Journal of International Studies* 8 (3): 112–127. http://dx.doi.org/10.14254/2071-8330.2015/8-3/9

Peker, S.; Tvaronavičienė, M.; Aktan, B. 2014. Sustainable risk management: fuzzy approach to volatility and application on FTSE 100 index, *Entrepreneurship and Sustainability Issues* 2(1): 30-36. DOI: http://dx.doi.org/10.9770/jesi.2014.2.1(4)

Rajnoha, R. Novák, P., Merková, M. 2016c, Relationships between Investment Effectiveness Controlling and Business Performance, *Montenegrin Journal of Economics* 12 (2): 29-44.

Rajnoha, R., Lesníková, P., Korauš, A. 2016 b. From Financial Measures to Strategic Performance Measurement System and Corporate Sustainability: Empirical Evidence from Slovakia, *Economics and Sociology* 9(4): 134-152.

Rajnoha, R., Štefko, R., Merková, M.,Dobrovič, J. 2016 a. Business Intelligence as a Key Information and Knowledge Tool for Strategic Business Performance, E + M Ekonomie a Management, 19(1): 183-203. http://dx.doi.org/10.1524.0/tul/001/2016-1-013

Schuh, S., Stavins, J. 2011. „How Consumers Pay: Adoption and Use of Payments". Federal Reserve Bank of Boston, Issue 122, pp. 135.

Šileika, A., Bekerytė, J. 2013. The theoretical issues of unemployment, poverty and crime coherence in the terms of sustainable development, *Journal of Security and Sustainability Issues* 2013 2(3): 59–70. http://dx.doi.org/10.9770/jssi.2013.2.3(5)

Snyman, C., R., Criminal Law, Third Edition), Durban: Butterworths, 1995, 487.

Stasytytė, V. 2015. Conceptualization of financial system sustainability, *Journal of Security and Sustainability Issues* 4(4): 391-402. http://dx.doi.org/10.9770/jssi.2015.4.4(6)

Štitilis, D., Klišauskas, V. 2015. Aspets of cybersecurity: the case of legal regulation in Lithuania, *Journal of Security and Sustainability Issues* 5(1):45–57. http://dx.doi.org/10.9770/jssi.2015.5.1(4)

Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016. Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197-210. http://dx.doi.org/10.9770/jssi.2016.6.2(1)

Štitilis, D.; Pakutinskas, P.; Malinauskaitė, I. 2016. Preconditions of sustainable ecosystem: cyber security policy and strategies, *Entrepreneurship and Sustainability Issues* 4(2): 174-182. http://dx.doi.org/10.9770/jesi.2016.4.2(5)

Sulphey, M. M.; Alkahtani, N. S. 2017. Economic security and sustainability through social entrepreneurship: the current Saudi scenario, *Journal of Security and Sustainability Issues* 6(3): 479-490. http://dx.doi.org/10.9770/jssi.2017.6.3(12)

Teivāns-Treinovskis, J.; Amosova, J. 2016. Some aspects of criminal environment impact on sustainable entrepreneurship activities, *Entrepreneurship and Sustainability Issues* 4(1): 17-24. http://dx.doi.org/10.9770/jesi.2016.4.1(2)

Teletov, A.; Nagornyi, Y.; Letunovska, N.; Shevliuga, O. 2017. Competitive and sustainable technological development: focus on business enterprises, *Journal of Security and Sustainability Issues* 6(3): 491-500. http://dx.doi.org/10.9770/jssi.2017.6.3(13)

Tumalavičius, V.; Ivančiks, J.; Karpishchenko, O. 2016. Issues of society security: public safety under globalisation conditions in Lithuania, *Journal of Security and Sustainability Issues* 5(4): 545-573. http://dx.doi.org/10.9770/jssi.2016.5.4(9)

Tumalavičius, V.; Veikša, I.; Načišcionis, J.; Zahars, V.; Draskovic, V. 2017. Issues of State and Society Security (Part I): Ensuring Public Security in the Fight against Crime, *Journal of Security and Sustainability Issues* 6(3): 401-418. http://dx.doi.org/10.9770/jssi.2017.6.3(7)

Virglerová, Z., Kozubíková, L., Vojtovič, S. 2016. Influence of selected factors on financial risk management in SMEs in the Czech Republic. *Montenegrin Journal of Economics* 12(1): 21-33.

Zinman, J., (2008). Debit or Credit, *Journal of Banking and Finance*, p. 19.