USE OF CUSTOMER HABITS IN DETECTION OF DIGITAL CHANNEL FRAUD

Erkut BALOGLU[1],Elif GUNEREN GENC[2]

[1]*Karaca Group as Customer Asistant General Manager, baloglue77@gmail.com,*
Orcid No :0000-0001-9613-8925
[2]*Istanbul Commerce University, Faculty of Business, elifg@ticaret.edu.tr,*
Orcid No: 0000-0001-5439-914X

Abstract

The purpose of this study is to investigate the use of channel usage habits of bank customers to detect channel fraud. If a bank can analytically understand the digital channel usage behavior of its customers, it can prevent fraud or cash outflows by taking advantage of the differences between the behavior of the fraudster and the customer in a potential channel/account hijacking case. The study examined the characteristics of transactions made by 950 customers of a widely used bank in Turkey in the channels and customer behavior. Independent variables such as the location where the customer logs into the digital channels, the password entry times during login, the time elapsed between two consecutive digital channel entries, the number of transactions made during a channel login, the number of active credits during channel use, the number of transactions made, the use of preset credit, and the frequency of digital channel use have been found to be statistically significant in distinguishing between genuine customers and fraudsters.

Keywords: Banking, Channel Usage; Fraud Prevention; Digital Channels

JEL Classification: G2; G21; 032

Introduction

Today, customer behavior is changing in line with new trends and technologies. Over the past 30 years, technological innovations and an increasingly competitive environment have led to significant changes in the banking sector. On the one hand, technologies such as image processing and OCR reduced paper-based processes, reduced costs, and centralized banking operations; on the other hand, alternative distribution channels were developed that allow consumers to access banking services from home and handle banking transactions on their own (Daniel& Storey, 1997). The biggest impact on the customer-bank relationship has been cell phones, which have made banking accessible regardless of time or place, and the advent of new-generation mobile devices with broadband networks has greatly changed customers' habits and preferences (Gigov & Popska, 2017). In response to customer expectations, banks offered mobile banking branches and set up extensive ATM networks to improve access to cash. With the rise of self-service banking channels, human application interface, experience in self-service channels, security, convenience, and cost efficiency influenced brand perceptions (Kumbhar, 2011). Banks' new channels and business models, customers' use of digital channels, and fraudulent activities increased, making it imperative for legal institutions and organizations to introduce new regulations and laws. The evolution that has taken place since the early 2000s in banks' internet and mobile branches has brought efficiency to the forefront, with cost pressures, smartphones, artificial intelligence applications, Big Data analytics technologies developed and increasingly deployed (Omarini, 2017). By 2008, banks had implemented two main business models to offer financial products and services to customers. The first was to diversify distribution channel products and services over the internet in addition to existing physical channels, and the second was to offer a fully internet-based banking service without physical branches (Arnaboldi & Claeys, 2008:12).

With the widespread use of smartphones and tablets, the way consumers interact with financial institutions also changed, shifting from branches to mobile channels. Thus, mobile devices have become a new tool for consumers to manage their financial transactions. Banks have also embraced this change, increasing interactions with customers via mobile channels, which has led to a shift in transactions to digital channels (Broeders & Khanna, 2015). With the successful adoption of internet banking and the widespread use of ATMs, customers using digital channels have begun to pay lower fees for banking services (Corbat & Kirkland, 2015). Thus, internet banking

has emerged as the most cost-effective method of providing financial services and promoting products (Karjaluoto, Pikkarainen, Pikkarainen, & Pahnila, S.,2004).

Digital Banking

In the literature, digital banking can be defined as the processing of transactions that can be made by physical bank branches via the internet without customers having to go to the branch (Karjaluoto, Pikkarainen, Pikkarainen, & Pahnila, S., 2004). Digital channels have two main features. The first is the electronic and paperless execution of payments, and the second is the accounting and reconciliation of the transaction in a central system (Shy & Tarkka, 2002).

For customers, internet banking means time, cost savings, and spatial independence (Karjaluoto, Pikkarainen, Pikkarainen, & Pahnila, S., 2004). In addition to the added value that digital banking services offer customers, reasonable transaction fees and pricing have a significantly positive impact on the customer experience. For this reason, mobile banking with cheaper transaction costs is becoming increasingly popular (Unyathanakorn& Rompho, 2014). Studies by Kumbhar in 2011 found that the human application interface is the backbone of banking services today. In the same study, experience and brand perception in self-service channels were found to be related to safety, reliability, responsiveness, convenience, and cost-effectiveness (Kumbhar, 2011). In their study, Gigov and Popska (2017) found that customers use self-service channels for simple transactions such as depositing and withdrawing money, and they showed that the mobile channel greatly changed customers' habits and preferences, especially after the advent of new generation mobile devices with broadband networks (Gigov & Popska. 2017).

While the use of digital channels is growing rapidly, some customers are avoiding the use of mobile channels. Reasons for the reluctance to use digital platforms include security concerns and the small screen size of cell phones makes them difficult to use (Liu, Abhishek&Li, 2015). In his 2019 study, Zhu mentioned that the screen size of the devices on which digital banking is used also affects the perception of security. He explained that the small screens on these devices meant customers were concerned about making mistakes when performing digital transactions and felt they could not access enough information about the transaction.

Fraud

According to the regulation on the internal systems of banks, operational risk is defined as the possibility of suffering damages that may be caused by the oversight of errors and irregularities as a result of disruptions in internal controls, the failure of bank management and staff to act in a timely manner and on time, errors in bank management, errors and disruptions in information technology systems, processes that do not function properly, people abusing the system and external factors. One of the activities in operational risk management is the "prevention of fraud attempts by individuals".

In its most general form, fraud is defined as the illegal use of a system. External fraud activity is observed in the use of credit cards, debit cards, internet banking accounts, and call centers (telephone banking) in banking. There may also be instances of internal frauds such as money laundering and personnel fraud (Duman & Ozcelik, 2011). Since this study will focus on preventing third-party fraud and channel fraud in particular, abuse and channel fraud will be examined in more detail at this stage of the study.

Channel fraud is defined as fraud carried out by phishing customers' passwords and making transactions on behalf of customers through banking channels while forced money transfer is when a customer transfers money or hands over money to the fraudster in cash through deception or intimidation over the phone.

Fraudsters have developed various methods to access credentials and passwords, such as phishing, fake websites (pharming), social engineering, SIM card replacement, hijacking users' mobile devices (phones, laptops, etc.), or exploiting data leaks (European Fraud Report 2019 - Challenges facing the payments industry)

Two of the most common methods for identity theft are phishing and phishing websites (pharming). While phishing is based on collecting personal information through mass email messages, fake websites are based on redirecting website traffic to another illegal website (Brody, Richard & Mulig, 2007).Phishing attacks aim to obtain individuals' information through mass email messages. It is generally used to learn a person's password, or

pilfer debit account or credit card information. A specially prepared phishing email appears to come from an official institution or as a genuine email. Using the fake email, users are directed to fake sites and reveal their information (Brody, Richard & Mulig, 2007).Another type of phishing attack is the SMS phishing method known as SMishing. This method uses short text messages instead of email. Content for phishing attacks is often structured around enticing fake scenarios such as gifts, discounts, salary rises, free vacations, prize money, or the like (Brody, Richard & Mulig, 2007).

The method of social engineering (vishing), on the other hand, is based on manipulating people into sharing their personal and/or financial information instead of technical knowledge and skills. In this method, the fraudster usually introduces himself as an employee of an official institution such as a bank, police or government agency and says things that prompt the user to act quickly, such as there is a suspicious transaction on the user's account, or the user is receive a refund or that his account information needs to be updated. After convincing users to share the confidential information they need, such as password, card number, and account number, they access users' accounts with the information they have and conduct illegal financial transactions (Fraud The Facts 2019 - UK Finance Report).

Using one of these methods, malicious individuals accessing personal information, login ID and password can use this information for numerous financial transactions such as shopping, making payments, seizing the affected person's accounts, applying for a loan on that person's name and transferring the money to various accounts (Fraud The Facts 2019 - UK Finance Report).

Literature Review

Illegal activities related to digital financial transactions are becoming increasingly complex and cross-border. Fraud results in large financial losses for both customers and banks. There are many studies in the literature on fraud detection using various data mining algorithms, including decision trees, regression models, and artificial neural networks. In credit card fraud, rule-based expert systems (Leonard, 1995), decision trees that measure similarity (Kokkinaki, 1997), logit regression algorithms that calculate the probability that a fraudster may be operating, and neural networks are commonly used for fraud detection. Dorronsoro (1997) developed a technically accessible online fraud detection system based on a neural classifier. Genetic algorithms are widely recommended as predictive methods to detect fraud. An algorithm proposed by Bentley (2000) was used to create rules of logic that can classify credit card transactions as suspicious and non-suspicious. Bolton and Hand (2002) propose two clustering techniques using peer group analysis and breakpoint analysis for behavioral fraud. Bayesian networks are also one of the fraud detection techniques applied to fraud detection in telecommunications (Ezawa & Norton, 1996) and credit card (Maes et al., 2002). There are models based on Bayesian learning algorithms that firstly identify a set of suspicious transactions and then run a Bayesian learning algorithm to predict fraud (Panigrahi, Kundu, Sural &Majumdar, 2009). There are models that identify patterns for normal card use and use association rule mining to identify the suspicious ones that do not fit these patterns (Sanchez, Vila, Cerda & Serrano, 2009). Artificial immune system algorithms, developed with biological metaphors, are built on eliminating fraudsters (pathogens) with negative selection, just like the immune system (Sorournejadı, Zojaji, Atani & Monadjemi, 2016). Assisted vector refers to algorithms designed to create vector planes that distinguish fraudsters from real customers by using machine learning and pattern recognition and regression techniques (Sorournejadı, Zojaji, Atani & Monadjemi, 2016).In evaluating these models, fraud detection rate, hit rate, and Gini index are among the popular performance measures for fraud detection (Gadi, Wang & Lago, 2008; Kim & Han, 2003).

Regardless of which model or method is chosen, it must meet certain conditions in fraud detection. The first of these is that the system must handle skewed data distributions because the number of fraudulent transactions is much smaller than the total number of transactions, or the data are split into training samples where the distribution is less skewed (Chan et al., 1997). The second is to understand in a very short time at the time of the transaction whether the transaction is fraudulent and to stop the transaction if necessary. To accomplish this task, which requires real-time data processing, instant access to the data used as input by the model, fast processing, and instant feedback capabilities are required (Abakarim, Lahby & Attioui, 2018). The third is the need for flexible adaptation. Since fraudsters are constantly inventing new techniques, the system must be adaptable and evaluated regularly.

Fraud prevention models can be inefficient in catching up with new fraud methods. Dynamic adaptation of the fraud prevention model to new fraud methods, remodeling and testing may take some time (Sorournejad1, Zojaji, Atani & Monadjem, 2016).Since classical algorithms are not sufficient to detect fraud due to the difficulties mentioned above, new algorithms or hybrid solutions should be developed (Duman & Ozcelik, 2011).

The aforementioned modifications of algorithms or the use of hybrid models should also take into account the behavioral patterns of fraudsters. For example, when fraudsters hack a card, they usually spend the entire available limit. According to statistics, they can reach the entire limit in an average of four or five transactions. Therefore, measuring the extend of damage caused by fraud is more important. In other words, detecting fraud on a card with a large usable limit is more valuable than detecting fraud on a card with a low available limit (Duman & Ozcelik, 2011). Fraud prevention models suffer from an ethical problem arising from their use. This technique can identify some customers as real customers, although they are actually fraudulent, and some real customers as frauds. From an ethical perspective, these errors should be minimized. However, it costs less to misclassify real customers as fraudsters than to misclassify fraudsters as real customers. To minimize costs, banks may do modellings that tend to classify customers as fraudulent. However, it would be unethical to reject genuine customers with the same characteristics as fraudulent customers (Delamaire, L., Abdou, Hah &Pointon, 2009).

In the ethical problem expressed by Delamaire, Abdou, and Pointon (2009), banks can keep thresholds high in their models, to detect fraudsters at a maximum level. For this reason, they can classify real customers as fraudulent and reject their transactions. However, this situation minimizes the costs not only for the bank, but also for the entirety of customers. If the fraudster is mistaken for a real customer, the customer loses money. Otherwise, a confirmation call is made and the transaction is allowed on the second attempt. When making a confirmation call, banks never use phrases that would characterize the customer as a fraudster, but rather confirm their identity and the transaction. This means that identity confirmation is done in a transaction where the customer is not considered a fraudster, and the communication language significantly reduces the ethical problem. The focus of fraud prevention in digital channels is relatively new in the literature compared to other fraud prevention topics. In the 2019 literature review conducted by Minastireanu and Mesnita (2019), only 9 of 50 literature studies address fraud in digital channels. In comparison, 38 studies are related to credit card fraud and 3 of them are related to financial document fraud (Minastireanu & Mesnita, 2019). This is illustrated in Table 1. It is important that the algorithm makes the right decision to minimize the ethical problem and have a minimal impact on customer satisfaction. Fast processing is critical to interjecting on a transaction. When algorithms are evaluated for decision accuracy, speed, and spread, Assisted Vector Machine Learning comes to the fore.

Tablo 1.Methods Used in Fraud Prevention

Type of technique	Number of articles	Decision accuracy	Coverage	Costs	Sum
Support Vector Machine (SVM)	17	3	3	3	9
Bayesian network	8	3	2	3	8
Fuzzy Logic based system	4	3	2	3	8
DBSCAN	2	3	2	3	8
Logistic regression	8	3	2	2	7
Decision Tree (DT)	19	2	2	3	7
K-nearest neigbor (KNN)	10	2	2	3	7
Artificial Neural Network (ANN)	20	2	2	3	7
Random forest	8	3	2	2	7
Naive Bayes	7	2	2	3	7
Self-organizing map (SOM)	4	2	1	3	6
Artificial Immune System (AIS)	4	2	3	1	6
Genetic Algorithm (GA)	13	2	2	1	5
Hidden Markov Model (HMM)	8	1	1	3	5

References: Minastireanu and Mesnita 2019

The advantages and disadvantages of algorithms were evaluated in the study by Sorournejadı, Zojaji, Atani, and Monadjemi in 2016. In this evaluation, it was found that assisted vector learning causes performance issues with high volumes of data and there are difficulties in understanding the transparency of the results and what parameters are involved in the decision making process. The same study mentioned the difficulty of constructing neural networks and interpreting their results, and noted that algorithm training for Bayesian networks took a long time. It is stated for fuzzy logic that it is very slow in detecting cheaters and also costly (in terms of information processing).

Implementation

Banks are seeing more customers use digital channels. As digital channels become more pervasive, channel and account theft fraud attempts increase, new methods based on phishing and deceiving customers are developed, and traditional fraud prevention processes begin to fail. The most important aspects of detecting channel fraud are logging into the channel and withdrawing money from the account. These two aspects are important to prevent fraud. According to USOM data, 700 phishing sites are opened per month in Turkey, which are shut down according to warnings from banks. The fraudulent success rate of phishing incidents is 1%. At least one customer is affected by each phishing attack, causing on average TRY 1,500 worth of loss per customer. Based on banks subjected to phishing attacks in Turkey, the loss is worth TRY 630,000/year per bank. More important than the loss of money is the loss of customers and the risk of losing the good reputation. (USOM and BKM)

The study examines the usage habits of digital channels that are the subject of the study. The study has two parts. The first part consists of studying the usage characteristics and behaviors of customers and fraudsters on digital channels, and determining what common and different behavioral characteristics they share when transferring money out of the bank both during and after logging into the channel. The second part is to research and compare analytical methods that can be used in warning mechanisms that can be created to prevent fraud based on these characteristics. The analysis procedure mentioned in the second part is a two-tier construct. At the first level, the probability that the person attempting to log into the digital channel is a fraudster is calculated based on the behavior, location, device, demographic characteristics, and method of logging into the channel, during the security process. At the second level, after logging into the digital channel, a customer's behavior in digital channels, the menus they click on, the first menu they click on, the first transaction, the transaction amounts, the location, demographic characteristics are used to determine the probability of a fraud attempt.

In this study, a model is built using the logit regression algorithm with panel data. Its contributions to the literature are twofold. Firstly, there is a new opportunity to transfer lessons learned from credit card fraud to digital channels. Using the panel data, it will be possible to identify the behavioral pattern of each customer and flag deviant behaviors from this pattern as possible fraudulent activity, as well as analyze the general behavioral patterns of fraudsters using all customer data. Secondly, fraud prevention algorithms that are generally used when logging into a digital channel continue to be used after logging into the channel to develop an understanding of preventing the outflow of funds.

Population and Sample

To understand a bank customer's access and usage habits to digital channels, the research was based on 70222 channel logins and usage log records of 950 randomly selected customers of banks with widespread branches in Turkey, which are ranked among one of the top 10 banks in terms of asset size. There are 114 fraud cases in these records, and the research is based on 2019 data. In addition, all customers have Personal Data Protection Act authorizations.[1]

950 customers were identified as "data set" while 114 customers exposed to fraud were identified as "defrauded". Also, Appendix 1 contains all the data in the data set.

[1] Personal customer data and financial data are masked by the bank. The research was done in an environment determined by the bank, and even masked customer data was not transferred outside the banking environment.

Table 2.Gender Distribution of Customers

Gender	defrauded customers	all customers
female	26%	25%
male	74%	75%

When Table 2 is examined, it is understood that 75% of the 950 customers are men, and 74% of the 114 customers who have been subjected to fraud are men.

Table 3.Segment Distribution of Customers

Segment	defrauded customers	all customers
Individual - Loan Customer	78%	69%
Individual - Deposit Customer	15%	18%
High Wealth Individual	2%	8%
Business Customer	4%	4%
SME/OBI	1%	1%

When Table 3 is examined, it is observed that 69% of them are individual customers who are loan debtors. It is observed that the ratio of retail customers with loan debts has increased to 78% among the customers exposed to fraud, while the ratio of highly wealthy retail customers is 2%.

Table 4.Age Distribution of Customers

Age	defrauded customers	all customers
18-24	15%	15%
25-34	25%	27%
35-44	24%	27%
45-59	27%	25%
60+	9%	6%

When the age distribution of customers is examined, a weighted distribution is observed for people who use banks intensively between 25-59. It can be thought that customers over the age of 60 are especially targeted by fraudsters, as it is easier for them to have deposits with their lifetime savings and because it is easier to be deceived over the phone.

Table 5.Distribution of Channel Entrance Units Based on Education Levels

Education	defrauded customers		all customers	
Unknown	23	5%	5.526	8%
Primary school	157	31%	8.382	12%
High school	23	5%	6.698	10%
Middle School	216	43%	28.348	40%
University and above	89	18%	21.268	30%

In Table 5, it is observed that fraud cases are concentrated in primary school graduates and decreased in university and higher individuals.

Table 6. Distribution of Customers Based on SMS Password Entry Times

Login Time - Password	defrauded customers		all customers	
0	84	17%	63397	90%
5 sec	255	50%	6131	9%
5 - 30 sec	85	17%	447	1%
30 sec - 1 min	54	11%	179	0%
1 - 2 min	20	4%	42	0%
2 min	10	2%	26	0%

In Table 6, the time for customers to enter the SMS passwords sent to them while logging into the digital channel has been examined. It has been determined that scammers enter passwords slower than customers. This happens because during the fraudulent activity, the fraudster spends extra time talking to the customer to obtain the password or copying the password over the virus.

Table 7.Number of Financial Operation During Channel Usage

Financial Operation	defrauded customers		all customers	
0	273	54%	48370	69%
1	152	30%	18527	26%
2	48	9%	2203	3%
3	16	3%	580	1%
4	8	2%	233	0%
more than 5	11	2%	309	0%

In 69% of the cases where a standard customer enters the digital channel, they exit the channel by simply viewing information without making any financial transactions. Scammers, on the other hand, view in 54% of the cases they access the digital channel. Also, scammers are more likely to take more than 3 actions on one login.

Table 8. First Process

First Process	defrauded customers		all customers	
Just Login to the Channel	235	46%	45482	65%
Transfer	57	11%	7957	11%
EFT	30	6%	3486	5%
Withdrawal with QR	26	5%	3313	5%
Credit Card Payment	22	4%	1225	2%
Paying bills	18	4%	876	1%
Deposit with QR	10	2%	678	1%
Other Payment	8	2%	582	1%
Consumer Loan Application	8	2%	459	1%
FX Buy/Sell	8	2%	379	1%
Other	86	17%	5785	8%

When all customers are examined in Table 8, the first financial transactions after entering the channel (if only observing and exiting) are money transfer or withdrawal. Then comes the payments. In fraudulent behavior, a consumer loan application is among the first transactions. In cases where the customer cannot find money in his account, the fraudster tries to use a loan. In addition, when the fraudster sees a time deposit account at the first login, he breaks the time account as the first transaction.

Model Structure and Hypotheses

There are 21 channel logins for each customer in the data set (when logging into digital banking). A balanced panel was created, with channel entries processed as time series and customers as cross-sectional data. As dependent variable with two levels it can be expressed as follows,

$$y_{it} = \begin{cases} 1, & \text{If the customer has been defrauded} \\ 0, & \text{If the customer has not been defrauded} \end{cases}$$

For the channel login model;

H1a: When logging into digital channels, genuine customers and fraudsters in significantly different ways.

For the Taking Money out of the Channel Model;

H2a: After logging into digital channels, genuine customers and fraudsters in significantly different ways with regards to behaviors and actions on the channel.

These are basically the two hypotheses.

Channel Login Model:

By using the panel logit model, a fraud attempt is estimated at the time of logging into the channel. Customer channel access data and demographic data were used as model-independent variables, and statistically non-significant variables were excluded from the model.

Tablo 9. Channel Login Model - Panel Logit

Dependent Variable: Fraud (1 or 0)

Independent Variables				
The customer's location at the time of entering the digital channel	-0.01673	(-0.00003)	0.0097222	*
OTP password entry time when entering digital channel	0.03002	-0.00006	0.0192078	*
Time elapsed between entering the digital channel and the previous	-0.00121	(-0.000002)	0.0005799	**
PC operating system used during login	0.00891	-0.000019	0.0030587	**
c	-6.19774		1.122.128	***
Rho	0.70981		0.04629	
Wald	2130.88	***		

Note 1. Figures besides estimated coefficients in parenthesis are marginal effects; besides marginal effects in parenthesis are standard errors. *,** and * indicates significance at 1%, 5% and 10% statistical levels respectively.**

Note2: According to the Hausman test results in the model, the random effects model was studied with robust standard studs since the presence of heteroscedasticitywas detected. Cross-section dependency was examined and it was determined that it does not exist..

When Table 9 is examined, the possibility of fraud exists if the location where the fraudster logs into the channel on behalf of the bank customer is different from the locations where the bank customer made login attempts in the past. Typically, bank customers log into digital channels from similar locations. These locations are indexed on the basis of districts. For successive logins from the same location, the location difference becomes 0. If login is made from another location, the location value is subtracted from 0 and takes on a value as negative as the district code. It can be seen in the model that location changes increase the probability of fraud and are statistically significantly related.

When accessing digital channels, banks send a one-off password to their customers via text message. Entering the password, directly from the text message, the customer logs into the digital channel. In case of fraud attempts, the password on this text message must be read by the defrauded customer or sent to the fraudster and entered by the fraudster. For this reason, password entry times in fraud cases are statistically and significantly longer than their entry by the customer. As can be seen in the model, the probability of fraud increases with increasing password entry time.

When fraudsters capture the customer's password and information, they log into the digital channel more than once. The first time they log in, they usually check the balance check and security settings, the security configurations, before exploiting the available funds and sending money on their next logins. Since the fraudster wants to quickly debit money from the customer's account, the time between channel logins tends to be shorter than the time between usual channel logins by the customer. Fraudsters try to pilfer as much money as possible by logging into an account on the same day and in succession. For this reason, the longer the time between logins, the lower the probability of fraud.

The operating system and version on the customer's personal computer using which he logs into the digital channel tends not to match the version of the operating system on the personal computer through which the fraudster logs into the digital channel on behalf of the customer. Matching operating systems are assumed to be 0. It was found that the difference in PC operating systems increases the probability of fraud.

Channel Usage Model:

After logging into a digital channel, the customer can perform various banking transactions, view the account balance or product features. Customers' digital channel usage habits differ from those of fraudsters. Based on behaviors and transaction patters within a digital channel, it is possible to distinguish a fraudster from a customer. If a fraudster is discovered to have infiltrated into the digital channel, the bank can still take action. It can be possible to prevent the money transfer or force the termination of the service being provided on the channel.
The results of the channel usage model, which will operate while the digital channel is in use to distinguish the customer from the fraudster, were interpreted both in terms of fraud prevention practices and statistically. The structure of the model was chosen, and after the model was set up, statistically significant variables were determined.

Tablo10. Channel Usage Model - Panel Logit

Dependent Variable: Fraud (1 or 0)

Independent Variables				
Channel entry model result	0.8587	(0.00243)	0.2769	***
Number of active credits of the customer	4.1426	(0.01173)	1.6949	**
Number of financial transactions at the customer's login	0.6370	(0.00180)	0.0901	***
Number of ready credits used at customer login	5.0428	(0.01428)	0.6489	***
Average number of sessions per month(i)	0.1627	(0.00046)	0.0342	***
Average number of monetary transactions per session(i)	-0.1273	(0.00036)	0.0276	***
c	-1.9141		1.8629	
Rho	0.75595			
Wald	135.72000	***		

(i): Last 6 months before Fraud
Note1: Figures besides estimated coefficients in parenthesis are marginal effects; besides marginal effects in parenthesis are standard errors. ***, ** and * indicates significance at 1%, 5% and 10% statistical levels respectively.
Note2: According to the Hausman test results in the model, the random effects model was studied with robust standard studs since the presence of heteroscedasticity was detected. Cross-section dependency was examined and it was determined that it does not exist..

Examining Table 10, it was found in the model that the probability of being exposed to fraud increases as the number of active loans increases while the customer is using the digital channel. This is explained by the fact that fraudsters try to take loans to create money for customers with zero account balances, and try to use credits after the first withdrawal of funds to get more money out of customers with money in their account balance.

The higher the number of transactions when using the channel, the higher the probability of fraud. While using the channel, fraudsters try to withdraw money from customers' accounts via wire transfer. The usual method is to transfer money into different accounts in small sums, not to attract unwanted attention and be subjected to extra checks. In addition, when the money in the account is depleted, a balance is established by using credit balances. All these transactions make it look as if the fraudster performs more transactions than a normal customer would while using the channel.

In the channel usage model, fraudsters and customers differ statistically and significantly in their tendency to use available limits. If it is a loan from an available limit, it becomes more likely that it is a case of fraud. Fraudsters want to quickly use credits in the name of the customer without entering any information. For this reason, they tend to use standing limits already allocated to the customer.

Customers who tend to use digital channels more often are more likely to be deceived. More logins into digital channels makes customers more exposed to fraud risks, making them more likely to be the victim of fraudsters. In addition, the result of the channel login affects the channel usage model of the model operating at the time of logging into the channel while the fraudster is being analyzed.

Results and Discussion

This study makes it clear that in this era of increasing digital channel use, marginal benefits in preventing channel fraud can be achieved if banks can better understand their customers' digital channel usage patterns analytically. The fraud cases included in the modeling data consist of fraudsters who have managed to circumvent banks' rule-based prevention and monitoring structures. Looking at the model results, it appears that a model that numerically separates fraudsters from real customers by taking customer behavior and usage habits as input can provide additional marginal utility for rule-based prevention systems.

In the event of a fraud attempt, the bank can exploit the differences between the fraudster's behavior and the customer's behavior to prevent the fraudster from logging into or leaving the digital channel.

The study found that the more the location changes, the longer the password entry times and the longer the PC is used as the operating system, the more likely it is to be exposed to fraud. The longer the time between logins to digital banking, the lower the probability of being defrauded. The likelihood of fraud was found to increase as the number of active loans, the number of transactions conducted, the use of loans with ready limits, and the frequency of digital channel use increased during channel use.

Article 36 of the "Regulation on Information Systems and Electronic Banking Services of Banks", published in the Official Gazette on March 15, 2020, and came into force on August 1, 2020, sets out the minimum requirements that banks need to fulfill to identify transactions with a fraud risk in electronic banking services. Regulators are recommended to include the use of models based on customer behavior in these minimum requirements.

APPENDIX

Appendix 1: Data

Data
Branch
Gender
Legal type
Customer age
Marital status
Segment
Number of addresses
Type of home address
Educational status
Customer's profession
How many seconds does it take to enter the OTP password when entering the digital channel?
From which province is the entrance to the digital channel made?
Time elapsed between entering the digital channel
Change of customer contact between two logins
Number of active deposit accounts at the moment the customer logs in to the digital channel
Channels used when entering the digital channel
Total assets (TL) of the customer at the time of login to the digital channel
Number of active credits at the moment the customer logs in to the digital channel
Total number of EFT / Remittance made during login to the digital channel
Total amount of EFT / Money Transfer made during login to the digital channel
Average number of sessions per month - Before Fraud Last 6 months
Monthly average monetary transaction amount - before fraud last 6 months
Monthly average number of monetary transactions - before fraud last 6 months

Average amount per session - prefraud last 6 months

Average number of monetary transactions per session - prefraud last 6 months

Customer's digital experience period (days)

What is the first action during this login?

Has the customer applied for a loan in this login?

Has the customer used ready credit in this login?

What method did he enter in this login?

The platform the customer uses at the time of login

References

Abakarim,Y., Lahby,M., Attioui A. (October 2018). An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning, *Conference Paper · October 2018,* DOI: 10.1145/3289402.3289530

Brody, R, Mulig, E., Kimball, V. (2007). Phishing, pharming and identity theft. Academy of Accounting and Financial Studies Journal. 11. 43-56.)

Broeders, H. and Khanna, S. (2015). Strategic choices for banks in the digital age. *McKinsey & Company, January*.

Corbat, M. and Kirkland, R. (2015). Citigroup on engaging the digital customer. *McKinsey & Company, June.*

Daniel, E. and Storey, C. (1997). Online banking: strategic and management challenges. *LongRange Planning, 30(6): 890-898.*

Delamaire, L, Abdou, HAH and Pointon, J.,(2009). Credit card fraud and detection techniques a review. USIR digital collection of the research output of the University of Salford.

Duman, E., Ozcelik, M., (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications*, 38, 13057–13063

Gadi, M.,F.,A., Wang X., Lago, A.,P., (2008). Credit Card Fraud Detection with Artificial Immune System, *International Conference on Artificial Immune Systems ICARIS 2008: Artificial Immune Systems pp 119-131*

Gigov, I. S., & Poposka K. (2017). Digital Transformation Of The Banking Sector In Republic Of Macedonia: State And Opportunities For Further Advancement. *Economic Development / Ekonomiski Razvoj, 19*(3), 103-119.

Karjaluoto, H., Pikkarainen, T., Pikkarainen, K. & Pahnila, S. (2004). Consumer Acceptance of Online Banking: An Extension of The Technology Acceptance Model.

Kumbhar V.M. (2011). Factors Affecting The Customer Satisfaction In E-Banking: Some Evidences Form Indian Banks, *Management Research And Practice Vol. 3 Issue 4 Pp: 1-1*

Liu, J., Abhishek, V., Li, B. (2015). The Influence Of Mobile Channel On Customer Behavior In Omni-Channel Banking Services, *Business Computer Science Published in ICMB 2015*

Minastireanu, A., Mesnita G., (2019).An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection*. Informatica Economică vol. 23, no. 1/2019.*

Omarini, A., (2017). The Digital Transformation in Banking and The Role of FinTechs in the New Financial Intermediation Scenario, *International Journal of Finance, Economics and Trade (IJFET)* doi:10.19070/2643-038X-170001

Sorournejadı, S., Zojaji, Z., Atani, R.E., Monadjemi A.H., (2016). A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective

Unyathanakorn, K., Rompho N., (2014). Factors Affecting Customer Satisfaction in Online Banking Service, *Journal of Marketing Development and Competitiveness vol. 8(2)*

European Fraud Report (2019) – Payments Industry Challenges

Fraud The Facts (2019) – UK Finance Report