The Credit Card Fraud

Yang Han[*]

Letter and Science Office, Davis Davis, United States

*Corresponding author: yhhhan@ucdavis.edu

Keywords: credit card fraud; Card-not-present fraud; Credit card application fraud; detection technique

Abstract: Today, mankind has entered the "age of technology mania". A large number of different technologies are being used in different fields, such as military use, medical care, and education. More and more people are fascinated by the use of these technologies. Computers can help people process large amounts of data and help them discover a lot of new knowledge. But these convenient new technologies also come with an increasing number of risks. The Internet has made it increasingly easy for people to have their personal information stolen. Artificial intelligence has caused more and more scientists to worry about the future. Computer viruses have become a nightmare for those who work with computers. In this article, we will focus on credit card fraud. We will categorize several main styles of credit card fraud and explain how these criminal behaviors affect our lives. We will also consider how people can protect themselves from these frauds

1. Introduction

The term "credit card fraud" came into existence with the birth of credit cards. It was used to describe “When an individual uses another individuals’ credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Further, the individual using the card has no connection with the cardholder or issuer, and has no intention of either contacting the owner of the card or making repayments for the purchases made [1-3]”. Since then, this crisis has continued to occur in all aspects of our lives. Along with our massive consumption, this crisis has become more and more serious. For example, on February 5, 2013, 18 people were charged in connection with an international $200 million credit card fraud scheme in which a criminal gang invented 7,000 fake identities to obtain tens of thousands of credit cards. This is one of the largest credit card frauds in US history. As these credit card fraud cases are becoming more and more common, different kinds of credit card fraud are being separated into different categories for people. People classify credit card fraud as Card-not-present (CNP) fraud, Credit card application fraud, Account takeover, Credit card skimming, and Lost or stolen cards. In this article, we will pay attention to categorizing credit card frauds and explain how people can protect themselves from these tricks. And we will also mention what people need to pay attention to some characteristics of different credit card fraud.

The scale of the credit card is huge, and this article collects the overdue amount, average credit per card, and the yearly increasing rate of total credit amount to present the fraud of credit cards.

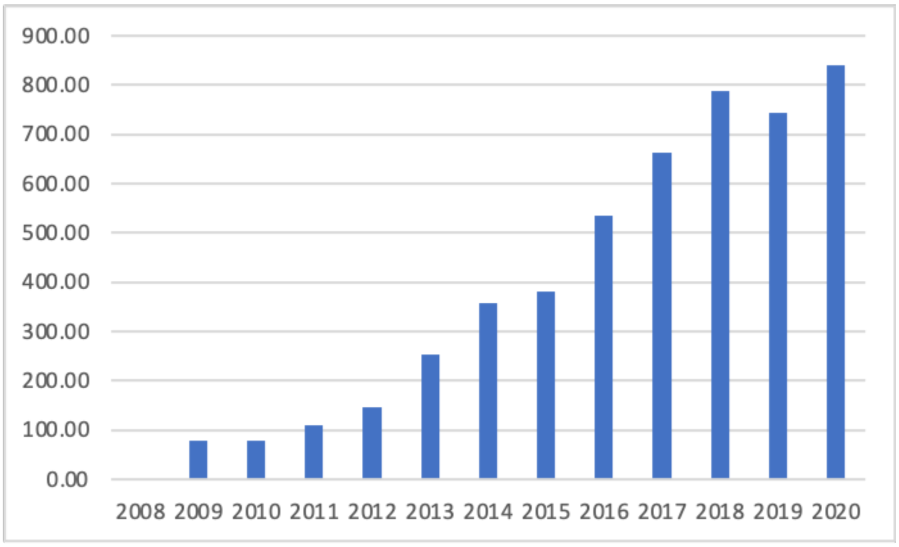

Figure 1. Total overdue amount of credit card

From figure 1, the total overdue amount of credit cards is increased exponentially from 2009 to 2020 generally. The amount rises from 7.6 billion yuan to 83.6 billion yuan within the decade.

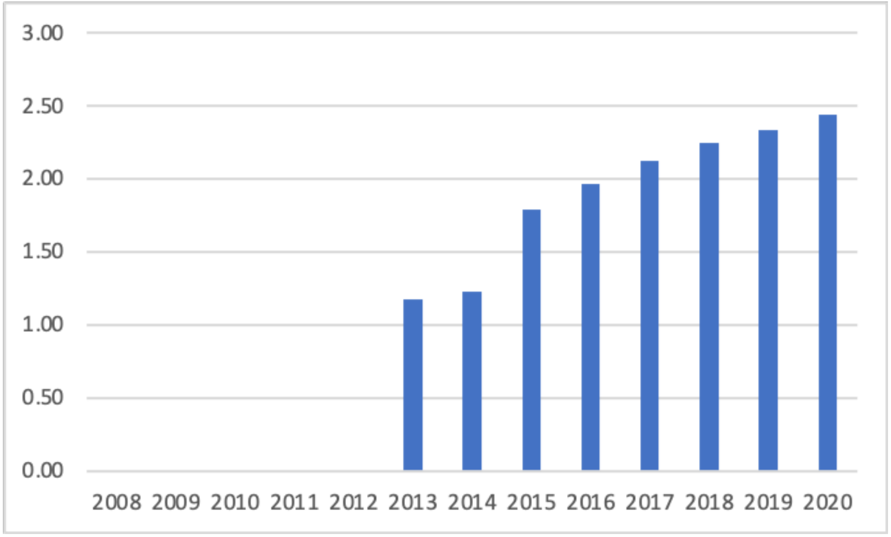

Figure 2. Average Credit per card

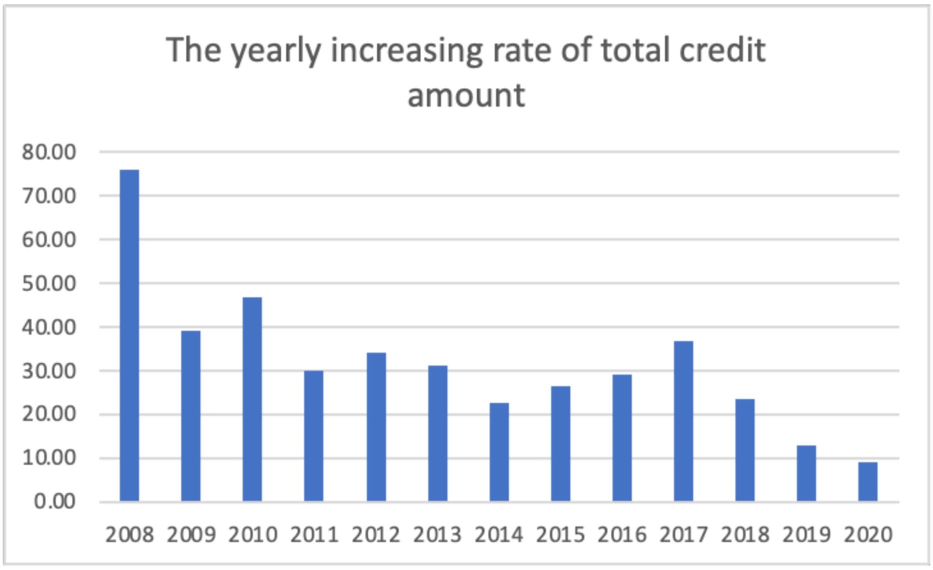

Figure 3. The yearly increasing rate of total credit amount

However, the average credit for each card is increasing more relatively, rising from 11k yuan to 24k yuan based on Figure 2.

According to figure 3, the yearly increasing rate of credit amount is around 30% from 2008 to 2017 but dramatically dropped to less than 10% in the following years.

In this article, we will split credit card frauds into 5 styles: Card-not-present (CNP) fraud, Credit card application fraud, Account takeover, Credit card skimming, and Lost or stolen cards. And in each subtitle, we will discuss these styles' traits and how to defend them

2. Card-not-present fraud

The definition of card-not-present fraud which we also called CNP is “Card-not-present fraud occurs in fraudulent transactions where a cardholder does not present a card to a merchant in person. It includes internet, phone, and mail-order transactions [4]”. In the paper called “Card- Not- Present Fraud- Challenges and Counteractions”, the author, Silvia Parushev, also expresses that “Card-not-present transactions will continue to increase their percentage and the reason for this is the unquestionable domination of payment cards in online commerce payments [5]”. Based on the development of people's payment methods, more and more people are using credit cards giving some unscrupulous people a larger base to commit fraud. In the article “What Is Card-Not-Present Fraud?” John Egan mentions that “Card-not-present fraud is increasing because some crooks have turned to card-not-present transactions following the rollout of more secure chip-enabled cards for card-present transactions." With the increase of credit paper, worldwide fraud is significantly increased. Like John says that “In recent years the percentage of card-not-present fraud in the total amount of fraud has been constantly growing in Europe and worldwide. Card-not-present fraud has emerged as a dominant category of fraud," Card-not-present fraud become a serious problem people faced. Based on this circumstance, it is important for people figuring out that how to stop this crisis. In Silvia Patrushev's paper, she lists an example solution about how to stop the Card-not-present fraud that is the "Shift rule for POS devices transactions” [6]. This rule began in 2015. The rules put the responsibility on merchants who are not EMV compatible. EMV, which we also called smart card, chip card, etc, is a kind of card that stores customers' data and reads by inserting it into a reader. Each card has its own pin number to prove its owner's identity to avoid the Card-not-present fraud.

3. Credit card application fraud

Based on the US law, the definition of credit card application fraud is mainly about “the unauthorized opening of credit card accounts in another person's name.” (legal information institute) Like Shiyang Xuan says in her paper named “Random Forest for Credit Card Fraud Detection”, that “Application fraud is that criminals get new credit cards from issuing companies by forging false information or using other legitimate cardholders' information [7-8]."Nowadays, people’s information become much easier to get by others through the internet. This leaves many people in a very precarious and dangerous position about their personal information and the credit card application fraud's rate becomes much higher than before. With the rise of Credit card application fraud, more and more attention is being paid to how to detect to prevent, and organize Credit card application fraud. Maheshwari provides 2 methods about his research about the Application side fraud that includes “Combination of communal detection and spike detection method” and “using Improved Sheep Flock Heredity algorithm” [9-12] Also, he uses Bayesian and neural network techniques to find out whether any frauds during the transaction about credit cards. He mentions that “While making the transaction with a credit card, the transaction is not accepted by trained HMM model with high probability, it is considered to be a fraudulent transaction.” [13] According to the paper called “Random Forest for Credit Card Fraud Detection”, Shiyang Xuan separates the 2 categories of fraud as application fraud and behavior fraud. She explains that “Behavior fraud is that criminals steal the account and password of a card from the genuine cardholder and use them to spend." She also explains the hidden marker model (HMM) to organize the model to figure out the sequence of transaction features in credit card transaction processing.

The following 3 subtitles are 3 different categories about Credit card application fraud. These 3 kinds of credit card application fraud are mainly not based on technology but rely on people's carelessness of people.

3.1 Account takeover

According to Selective Graph Attention Networks for Account Takeover Detection, Jialing Tao defines the account takeover as a type of fraud in which other people use unauthorized access to control the original owner’s account and it accompanies by account abuse, identity theft, etc. [7] The author lists an example about one of the largest online platforms, Alibaba. Alibaba as a big platform will always face a lot of fraudulent activities. Among these activities, the account takeover is the beginning of other kinds of fraud like coupon abuse, counterfeits, and so on. To solve this problem, Alibaba invests a huge amount of money for detection and use graph attention mechanisms within the sequence. And the author organizes research about the detection. The research includes a context graph for node embedding, the comparison models, and so on. At the end of his research, the author shows his confidence about selective graph attention mechanism within the sequence is a good way to solve the crisis about account takeover about online platform.

3.2 Credit card skimming

The case about credit card skimming is mainly about the people who use Credit card skimmers to practice theft. According to the article named “What Is a Credit Card Skimmer? And How You Can Protect Yourself” from Us News, the author John Egan describes that after a credit card skimming device reads the magnetic stripe on your credit, hackers can use these data to make fraudulent charges online or over the phone, sell your data, or create counterfeit cards.[14]. In the paper called “Keep Your Credit Cards Safe From Skimmers”, the author Robert Vamosi also shows his worries about Credit card skimming. He thinks the Pay at the Pump and ATMs Problematic are 2 main places that people will be stolen about their card information. The pumping stations are mostly automated in the United States and these stations become the easiest place for people embedding skimming devices in them late at night. These devices are very hard to be recognized by people and can get customers’ card information easily. ATMs Problematic is mainly about the exposed ATMs. Because no one monitors these machines, criminals can easily put their card skimmers on these machines to steal others' information. Under these circumstances, Robert Vamosi suggests that using credit cards is a kind of compromise because credit cards are protected by the law of zero liability programs and the bank will easily detect fraud actions through the internet but the debit card will not have these kinds of authority.

3.3 Lost card and Stolen card

Lost cards are, as the name implies, cards that have been lost or stolen and used by others to form a scam. According to “Lost, Stolen or Skimmed”, the author Trevor Budhram expresses that "Combined, these two categories constituted the highest percentage card fraud incidents in South Africa in 2007/2008 (68%). It further constituted the highest card fraud losses in South Africa on RSA issued cards year on year between 2005 and 2008 (57,1m in 2005/2006, R122,9m in 2006/2007, R150m in 2007/2008, and R33,1m in 2008/2009)." From these numbers, we can figure out that during that time the lost card and stolen card stand a high rate of fraudulent. But as Trevor says that “the use of this fraud type decreased by 60% in 2010.16 This was attributed to the roll-out of the chip-and-pin card". The appearance of pin number let people can not use lost or stolen cards to fraud [15].

4. Conclusion

Based on the above papers, some authors conclude some specific methods are more efficient than other methods for analyzing the data set. Fears Sayah uses exploratory data analysis to design bar charts, line parts, and so on to express his conclusion that XG Boost and cat Boost are more efficient than other methods. But datasets are different from one another and using different methods may lead to different accuracy and results. From Credit Card Fraud Detection with RF, Gabriel Preda utilizes functions data and correlations and many methods to conclude that the calculated accuracy is not very relevant since there is a great unbalance between the number of fraud and non-fraud. Whereas the ROC-AUC is very good using the default RF algorithm without any tuning. But the accuracy is not very relevant in the cases where there are a great unbalance between the number of fraud and the number of non-fraud events

There are various detection techniques including Decision Trees, Genetic algorithms, Clustering techniques, Neural networks. These techniques can be used to build scoring models suitable for each fraud case. For different cases, we may need different methods. But in general, RF is a good option considering sensitivity, precision, and accuracy. Whereas boosted tree model may perform well in credit card fraud detection. All in all, we may use different methods in different situations after tuning, it may depend on the data set itself.

However, the present researches do not take into account the classification of the different dataset and which method should be used for different datasets. And the scoring methods are generally considering accuracy alone. We may dig into the datasets and find their balance or other characteristics to suit different models or techniques.

References

[1] Tej Paul Bhatla, (2003) Understanding Credit Card Frauds “https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Bhatla.pdf”

[2] U.S. Attorney’s Office (2013) Eighteen People Charged in International, $200 Million Credit Card Fraud Scam “https://www.justice.gov/usao-nj/pr/eighteen-people-charged-international-200-million-credit-card-fraud-scam”

[3] Silvia Parusheva (2015) CARD-NOT-PRESENT FRAUD – CHALLENGES AND COUNTERACTIONS “https://www.researchgate.net/profile/SilviaParusheva/publication/279448751_CARD-NOT-PRESENT_FRAUD_ _CHALLENGES_AND_COUNTERACTIONS/links/5592e7d308ae16f493ee4722/CARD-NOT-PRESENT-FRAUD-CHALLENGES-AND-COUNTERACTIONS.pdf

[4] John Egan (2019) What Is Card-Not-Present Fraud? “https://creditcards.usnews.com/articles/what-is-card-not-present-fraud”

[5] Legal information Situation Credit Card Fraudhttps://www.law.cornell.edu/wex/credit_card_fraud

[6] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang and C. Jiang, (2018) "Random Forest for credit card fraud detection,” https://ieeexplore.ieee.org/abstract/document/8361343/

[7] J. Tao, H. Wang and T. Xiong, (2018)"Selective Graph Attention Networks for Account TakeoverDetection," https://ieeexplore.ieee.org/abstract/document/8637408?casa_token=vf_xRAs6ifQAAAAA:zbjSo8ee1UwQuJmYr3wwrx8G8NL5HI8U0CGiNeC648VP2FvZ4ijmh50gm6kAiFM2WIoUzr-g7S0

[8] V. Mareeswari and G. Gunasekaran (2016), Prevention of credit card fraud detection based on HSVM, https://ieeexplore.ieee.org/abstract/document/7518889 Credit card skimming

[9] Robert Vamosi (2010) Keep Your Credit Cards Safe From Skimmers “http://joeylemmens.be/competenties/jaar2/engels/Keep%20Your%20Credit%20Cards%20Safe%20From%20Skimmers%20-%20Schema.pdf”

[10] T Budhram(2012) Lost, stolen or skimmed: Overcoming credit card fraud in South Africa“https://www.ajol.info/index.php/sacq/article/view/101414”

[11] FARES SAYAH (2021) Credit Card FraudDetection ANNs vs XGBoost "https://www.kaggle.com/faressayah/credit-card-fraud-detection-anns-vs-xgboost"

[12] GABRIEL PREDA (2021) Credit Card Fraud Detection with RF (AUC=0.93) "https://www.kaggle.com/gpreda/credit-card-fraud-detection-with-rf-auc-0-93"

[13] Delamaire, Linda （2009） Credit card fraud and detection techniques: a review "http://eprints.hud.ac.uk/id/eprint/19069/1/AbdouCredit.pdf"

[14] SiddharthaBhattacharyya (2010) Data mining for credit card fraud: A comparative study "https://www.sciencedirect.com/science/article/abs/pii/S016792361 0001326"

[15] Jiaxin Gao (2019) Predicting Credit Card Transaction Fraud Using Machine Learning Algorithms "https://www.researchgate.net/publication/335139727_Predicting_Credit_Card_Transaction_Fraud_Using_Machine_Learning_Algorithms?_sg=jOqV3C3rGJOi_RVI84Q-Q0eDy62YDoTHFDHETdD44YNgDXDk4znG7mmIOEfwByUQDVc2nVFCY22x0mvZEEY1aHHp1ri7GZb739uvzWW.iOcyjPq3dIbMoiSwCkwM5EECYomi_VlFW5PTfovWCBP3Zv0zhTTzZ6NnH_Fto6Qi9XwxyCxb20LpO773GnyqmQ"