CREDIT CARD FRAUD

Lecturer PhD. Lăcrămioara BALAN
Lecturer PhD. Mihai POPESCU
Ştefan cel Mare University of Suceava, Romania
mihaip@seap.usv.ro

Abstract:
Credit card fraud is the misuse of a credit card to make purchases without authorization or counterfeiting a credit card. Credit cards are the most often used electronic payment instrument. Types of **credit card fraud are: online credit card fraud,** *advance payments, stolen card numbers,* **shave and paste, de-emboss/re-emboss etc.** *If current growth rates continue, credit cards and debit cards will each exceed the number of paid checks before the end of the decade. As the industry continues to expand and offer credit to more and more consumers, fraud will also grow.*

Key words: credit card fraud, prevention, smart card, internet

JEL Classification: E59

1. INTRODUCTION

Credit card fraud is the misuse of a credit card to make purchases without authorization or counterfeiting a credit card. Credit cards are the most often used electronic payment instrument. If current growth rates continue, credit cards and debit cards will each exceed the number of paid checks before the end of the decade. As the industry continues to expand and offer credit to more and more consumers, fraud will also grow.

Credit card fraud is successful because the chances of being caught are small and prosecution is very laborious.

2. ONLINE CREDIT CARD FRAUD

The lack of face-to-face or voice interaction on the Internet makes fraudsters more daring by providing them with anonymity, which makes the detection and prevention of online frauds more difficult. Lists of stolen credit card numbers are also being posted on the Internet or sold in newsgroups and can be used by a variety of individuals to purchase goods online without the authorization of the credit card's owner.

Credit Card Schemes

There are many different types of credit card schemes including selling the cards to thieves, family members using the credit cards without authorization, and fraudulendy obtaining a card. Statutes relating to the misuse of credit cards generally prohibit the obtaining of property or services through.

Fraudulent activity normally occurs within hours of the loss or theft, before most victims have called to report the loss. Increasingly, victims aren't even aware that their credit cards are being fraudulently used until they receive their monthly statement. It is extremely important that victims report the loss or theft of their card within 3 days, as they will not be held responsible for any charges that occur during that time frame. If the credit card company is not notified of the theft and the card is used, the customer will be liable.

Organized Crime Rings

Nigerian rings are especially notorious for stealing credit card and bank information from the mail. These articles are used to generate false identification documents, such as driver's licenses and Social Security cards. The credit cards themselves are duplicated and distributed to members of the rings. The false IDs are then displayed during purchases made with the stolen cards. Members of the ring go on spending sprees, ending only when the credit has dried up or the legitimate owner

reports their card as stolen. Often, counterfeit and stolen cards are express-mailed to members of the ring in other parts of the country.

Advance Payments

Consumer regulations require credit card issuers to credit customers' accounts immediately upon receipt of payment. This means deducting from the balance of the account before the check or other payment instrument has actually cleared the bank. A loophole such as this is easily exploited by experienced fraud rings.

Using a forged or counterfeit check, an advance or overpayment is made on a stolen credit card. Since the issuer must credit the payment at the time it is made, there is no time to verify the authenticity of the check. Consequendy, cash advances and purchases can be made immediately. This scheme can be extremely lucrative to the perpetrators.

Stolen Card Numbers

The Internet has become a breeding ground for individuals to obtain stolen credit card information. The thieves who steal this information find credit cards or lists of credit card holders and the corresponding numbers to their accounts. They then make the numbers available to a larger group which uses the information to obtain goods and services in the name of the cardholder. Wrongfully obtained information may be posted on websites that originate in foreign countries. The international nature of the fraud makes it arduous to deter or punish. A recent report involved a Romanian website that displayed stolen credit card numbers of more than 450 individuals, most from the United States. The list contained identifying information of cardholders and was available for several weeks before being shut down.

Shave and Paste

Any number of alpha or numeric characters is sliced from the card surface and other characters are attached to the card surface, utilizing fast drying epoxy-type glues. This might be done to put an entirely different but valid account number on the card or to change the name.

De-Emboss/Re-Emboss

In this scheme, the credit card is exposed to heat, usually from a household iron, a candle, or hot water in the microwave. Plastic cards, comprised primarily of polyvinylchloride, become more elastic when heated, and the embossed alpha/numeric characters are removed. An embosser puts new numbers and names on the cards. This process will generally create a "ghost image."

Counterfeit Cards

The fastest growing type of bankcard fraud involves the illegal counterfeiting of credit cards. Known as "white plastic" cards, this scheme utilizes credit card sized plastic with account numbers and names embossed on the card. This scheme works in conjunction with a corrupt and collusive merchant or a merchant's employee. Other counterfeit cards are manufactured from scratch using high speed printing facilities and used in association with organized crime groups. Manufacturing facilities have been traced to the Far East. The actual counterfeiting process has been immeasurably eased by new technology which allows more accurate duplication. Duplicating legitimate cards is still an intricate operation, however. Magnetic strips, numbers, holograms, and logos must all appear authentic. Desktop computers, embossers, tipping foil, and laminators are common tools in the reproduction process. Perhaps most difficult of all to accurately reproduce, however, is the hologram.

Telephone/Mail Order Fraud

The fraudster might offer a free trip or other nice prize, with the only catch being that the wanner must have a credit card. Once the thief has the number, he can order merchandise or have money wired to himself.

A great deal of credit card fraud is childishly simple to complete. Many crooks have great success by simply selecting a name from the phone book, calling, and pretending to be a Visa/MasterCard representative. The victim is told that his or her card number may have been obtained and used illegally by criminals. Or, a representative of a travel agency may call, claiming the victim has won a discount travel package. In any case, the victim is asked to read the card

number off for verification or inclusion in the discount deal. A surprisingly large amount of people fall for this scheme and give out their credit card information. Purchases through catalogues and mail orders are then often made using the victim's card number. They may select an unoccupied address to which their merchandise can be delivered, perhaps leaving a note asking the deliver service to simply put the package by the back door.

Mail Theft

A thief may steal credit cards already applied for by a bank's customer and issued by the bank. The thief will then attempt to use the card by posing as the intended recipient.

False Applications

Perpetrators might apply for a new card using information stolen from a wallet, purse, or the trash; or stealing a pre-approved credit card application out of the mail or trash. Also "take-one" applications that are prominent in stores offering credit cards to the public are ripe for fraud.

Credit "Doctors"

Credit doctor is the term used for fraudsters who sell stolen credit card account numbers via newspaper ads to people unable to get credit cards.

True Name Fraud

New credit card accounts can be opened by individuals possessing a victim's true name identification such as a driver's license or Social Security number. The true identification was either obtained as a secondary objective in the commission of a more aggressive offense such as robber}' or as the primary target of a lesser crime such as pick pocketing.

Non-Receipt Fraud

A form of credit card fraud in which the perpetrator intercepts credit cards that are in transit between the credit issuer and the authorized account holder. Losses attributable to mail theft have declined significantly as a result of "card activation" programs, where the cardholder must call their financial institution and confirm their identity before the card is activated.

Creditmaster

This software program, downloadable from the Internet, allows the user to produce valid credit card numbers. Counterfeiters can then put these numbers to use in phony cards.

Probing

The fraudster sets up a computer program that lets him run stolen numbers through various financial institutions in the hopes that one of them will still honor the number. Numbers that clear are often sold en masse to counterfeiters.

Skimming

Credit card skimming is more frequent in businesses where an employee must leave the customer's presence in order to run the transaction. A restaurant patron, for example, hands his credit card to a waiter who swipes the card into a wedge while conducting the legitimate transaction. Once the waiter has collected enough numbers, he can either sell them to a counterfeiter or simply produce his own fake cards using the stolen information. It may be months before the customer notices phony transactions on his statement, making the point of loss very difficult to determine. It follows that the guilty waiter is, therefore, unlikely to get caught. Skimming can also occur by tupping into a line used to transport credit card data.

Pretext Calling

Some fraudulent actors will call unsuspecting customers and pose as bank or credit card agents. The actor will request account information or other identifying information from the victim and use the information to apply for additional credit cards or to use the credit cards to purchase goods or services.

Account Takeover

The fake actor may take over a victim's account by requesting a change of address on the account and then calling to report the card lost or stolen. The issuing bank will then send the replacement card to the new address.

Institutional Identity Theft and "Spoof,, Sites

Fraudulent actors may create false Internet sites, pretending to sell goods to buyers who must enter their credit card information and other personal information in order to make purchases. The "seller" then uses the information to make fraudulent purchases in the name. of the buyer. More recently, fraudulent actors have begun creating "affiliate" sites of actual sellers or other creditors, such as banks. The perpetrator of the fraud then sends e-mails to existing customers of the actual seller or creator. These e-mails inform the unsuspecting customer that there is a problem with his or her account and asks the customer to log on to the site of the company that the wrongdoer has copied and to re-enter their personal and credit card information. The fraudulent actor then uses the information to make purchases.

Prevention

Prevention is the key to reducing credit card losses. Several programs can and are in place to reduce losses. Some of them are:

Education Programs

Tellers and merchants should be trained to be familiar with the security features of the credit card. Although the majority of counterfeit cards contain some of the security features, they usually are not complete and offer indicators that the card is not legitimate. Credit card issuers should take measures to inform their customers about credit card fraud, what the financial institution is doing about fraud, and how the consumer can help.

Liaison with Law Enforcement

Companies should develop strong liaison with law enforcement. When a company receives intelligence of hot frauds, law enforcement should be notified immediately.

3. FINANCIAL INSTITUTION MEASURES

Banks and other financial institutions have great resources at their disposal to prevent fraudulent transactions. Many of them need merely to enforce their existing policies.

- New account screening—educate personnel to thoroughly check applicants' information, comparing ID information, addresses, and credit reports for accuracy.
- PIN activation—bank customers are often required to provide personal identification numbers in order to activate their cards over the phone. Callers who are not able to provide the PIN number may have manufactured or stolen the card in question.
- Caller ID—most people calling to activate their card will do so from home. If the number on Caller ID does not match any of the telephone numbers listed in the customer's account information bank personnel should ask some identifying questions.
- Smart Cards contain a microprocessor memory chip instead of holograms. These cards are able to identify the user through encrypted information on the chip, and must be inserted into a "card reader" attached to the computer. That means the card cannot be used unless the purchaser is currendy holding it. A pin number is also required for the card so the thief needs to physically have the card and the security code in order to use it. This allows cardholders more purchasing options as well as increased security.

CONCLUSIONS

Judging from the past, credit opportunities for consumers will increase over time and, consequendy, more will fall victim to fraud. In the future, the trend will be one card for all types of financial transactions. Prototypes are currendy being developed and tested by the major credit card issuers. Fraud rings will adjust accordingly and new counterfeiting methods will emerge and law enforcement and investigators must maintain a global look when facing this type of fraud.

BIBLIOGRAPHY

1. Albrecht, W. Steve. Fraud Examination. Mason, Ohio, Thomson South-Western, 2003.
2. Androphy, Joel M. White Collar Crime. New York: McGraw-Hill, Inc., 1992.
3. Antle, Rick And Stanley J. Garstka. Financial Accounting. Cincinnati, OH: South-Western, 2002
4. Bintliff, Russell L. White Collar Crime Detection and Prevention. Englewood Cliffs, New Jersey: Prentice Hall, 1993.
5. Bologna, Jack. Handbook on Corporate Fraud. Boston: Butterworth-Heinemann, 1993.
6. Bonner, S.E., Z.V. Palmrose, And S.M. Young. Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases, The Accounting Review 73. October, 1998.
7. Cioclei, V., Manual de criminologie, Ed. AII Beck, Bucureşti, 2001.
8. Ciopraga A. - Criminalistica- Tratat de tactică, Ed.Gama, Iaşi, 1996.
9. Ciopraga A., Iacobută I. - Criminalistica, Ed.Junimea, Iaşi, 2001.
10. Carjan L. - Tratat de criminalistică, Ed. Penguin Book, Bucureşti, 2005.
11. Carjan L. - Criminalistică şi ştiinţe de contact, ed. a Il-a revăzută şi adăugită, Ed. M.A.I., Bucureşti, 2006.
12. Colectiv - The Code of Codes, Harvard University Press, SUA,1992.
13. Costescu I., Introducere în informatică, curs condensat, Universitatea din Bucureşti, 2003.
14. Dincu A. - Criminologie, Ed. Şansa, Bucureşti, 1995
15. Saferstein R. - Criminalistics: an introduction to Forensic science, Englewood Cliffs (publish.), N.Y, Prentince Hall, 1995.
16. Stancu EM. - Tratat de criminalistică, Ed. Actami, Bucureşti, 2001.
17. Şaguna, Dan Drosu, Tratat de Drept financiar şi fiscal, Ed. All Beck, Bucureşti, 2001.
18. Toffler A. - Powershift, Ed. Antet, Bucureşti, 1995.
19. Wold, Geoffrey H. And Robert F. Shriver. Computer Crime: Techniques for Preventing and Detecting Crime in Financial Institutions. Rolling Meadows, IL: Bankers Publishing Company, 1989.
20. Weston, Paul B., Kenneth M. Wells. Criminal Investigation: Basic Perspectives, 6th Ed. Englewood Cliffs, NJ: Prentice Hall, 1994.
21. Whidock, Charles R. Easy Money. New York: Kensington Books, 1994.