Credit Card Fraud (June 2008)

Credit card fraud is the unauthorized use of a credit card with the purpose of obtaining anything of value with the intent to defraud.

How It Happens

Credit card fraud is a problem that affects the entire consumer credit industry. It is one of the most common types of fraud and also one of the most difficult to prevent. According to the Federal Trade Commission (FTC), credit-related complaints have consistently ranked among their top 10 complaints for many years. In fact, some organized crime rings and even drug dealers have shifted criminal career paths to engage in this simple, lucrative, and relatively safe form of crime.

Credit card fraud can occur in person or via the Internet. Most consumer action groups, police departments, retail stores, and agencies, such as Better Business Bureaus (BBB) and the FTC, routinely release information for consumers on how to avoid credit card fraud and identity theft. Nevertheless, there are numerous forms of credit card fraud that are committed by enterprising thieves, organized rings, business owners, and even otherwise legitimate cardholders.

One method of obtaining account information or even an actual credit card is through postal theft. Other methods that have proven surprisingly effective in obtaining personal information include impersonating a card or application verifier via telephone, obtaining copies of past bills, or utilizing on-line directories. In some situations, offenders are also able to take advantage of contacts within the various credit bureaus to obtain legitimate bankcard account information for counterfeiting or telephone order purchasing. After having illegally obtained legitimate cards or account information, offenders then create fictitious identification including driver’s licenses, social security cards, and other materials to aid in the commission of credit card fraud.

Once the information is obtained, there are several forms of fraud that can occur. One popular type of credit card fraud is the advance payment scheme. This scheme utilizes counterfeit or stolen credit cards. The offender either makes an advance payment on the card or overpays an existing balance with a fraudulent check. Since the account is credited upon receipt of payment, cash advances can be immediately withdrawn before the payment check has cleared. Through numerous payments on numerous cards, an offender can realize large profits within a relatively short period of time.

Another type of credit card fraud involves the illegal counterfeiting of credit cards. New technology has aided criminals in producing exact replicas of existing cards and in creating fraudulent cards including the so-called “hidden” counter-measures. Illegal counterfeiting may be primarily responsible for the overall upsurge in credit card fraud.

Counterfeiters also buy and sell magnetic strips to produce fraudulent credit cards. The magnetic strips are essential because they contain names, account numbers, credit limits, and other information for legitimate or contrived Visa/MasterCard holders. By using a desktop computer system, source material, and
peripheral equipment, a counterfeiter can produce a fraudulent bankcard with relative ease. As technology has improved, counterfeiting credit cards has become a multi-step process. These steps can often include using desktop computer systems and peripherals such as laminators to produce more realistic looking cards. The counterfeited cards come complete with a hologram and fully encoded magnetic strip. Most of the supplies used to manufacture counterfeited bankcards, including the plastic cards and Visa/MasterCard holograms (the Visa dove and the MasterCard interlocking globes) are smuggled into the United States from the Far East.

Costs and Statistics

- It is estimated that the global rate of credit and charge card fraud is seven cents for every $100 transaction. Illegal credit card purchases totaled $788 million in the United States alone for the year 2004, representing 4.7 cents of every $100 worth of total purchases. Similar estimates have been reported in Great Britain, where it is estimated that £535.2 million were lost due to credit card fraud in 2007. In addition, Australia loses an estimated 4 cents per every $100 transaction to fraud.

- According to estimates, over 229 million records containing individuals’ identifying information have been compromised by data breaches since 2005. Although it is difficult to estimate or predict the number of compromised records that will be or may have been utilized for perpetrating fraud, the sensitive nature of the information contained within these records harbors the potential for increasing credit card fraud losses. Estimates of monetary amounts lost from data breaches can reach hundreds of millions of dollars.

- The Federal Trade Commission reports that victims’ information was used to perpetrate credit card fraud in 23% of the cases brought to the attention of the Identity Theft Clearinghouse in 2007. Of online credit/debit card fraud, the Internet Crime Complaint Center (IC3) reports that this type of fraud ranks 4th in the types of fraud committed over the Internet, compromising 6.3% of complaints reported to the IC3 in 2007.

- A report issued by Cybersource shows that, according to a 2007 survey of both small and large online businesses, 1.4% of all online revenue was lost due to payment fraud, with an estimate of $3.6 billion in losses for 2007. Additionally, the survey found that 1.3% of all accepted orders resulted in fraud losses. The median fraudulent order was $200 versus a median of $120 for legitimate purchases. Those retailers which also accept orders not located with the U.S. or Canada reported that international orders were rejected at a rate approximately 2.5 times higher than U.S. and Canadian orders due to suspicion of fraud. Overall, merchants rejected 4.2% of total orders on suspicion of fraud.

Examples/ Case Studies

- In February, Sharif J. Reid pleaded guilty to one count of conspiracy to commit credit card fraud and one count of credit card fraud. Reid admitted to taking part in a 17-month conspiracy with other individuals to use counterfeit credit cards. In a September 2007 search by law enforcement officials, nearly 100 counterfeit cards, two cash register rolls with approximately 1,800 additional credit card numbers, counterfeit drivers’ licenses, a document shredder, and a bag of shredded credit cards, and approximately $300,000 in electronic equipment, gold and diamond jewelry, and designer clothing was seized from Reid’s residence. Reid also admitted that he and another individual, Nandasharie Shivmangal, deposited over $500,000 in cash into their personal accounts from April 2006 through September 2007. As part of his plea agreement, Reid is to forfeit $700,000 related to the frauds. The conspiracy count carries a penalty of up to five years in prison and a $250,000 fine; the credit card fraud count carries a penalty of up to 10 years imprisonment and a $250,000 fine.
• Three individuals have recently been indicted for their involvement in a credit card mastering scheme. Steve Allen Black, Ronald Edward Black, and Dereck Lorenzo Dunston, all of Evington, VA were charged in a 25 count indictment related to the scheme in which legitimate access device account numbers were coded onto counterfeit access devices (credit cards). According to the indictment, the accused would meet individuals at a car wash in Lynchburg and either follow or ride with the individuals to local gas stations where the accused would use the pay-at-pump feature, swiping one of the counterfeit credit cards in order to pay. In return, the individuals would pay the accused half of the cost of the merchandise or gasoline in cash. Locally, the accused were known as the “Gas Men.” Beginning in April 2007 and ending in January 2008, the accused used more than 500 fraudulent credit cards to commit more than 3,000 fraudulent transactions, resulting in over $131,000 in charges. If they are convicted on all counts, each of the accused will face over 60 years in prison and nearly $2 million in fines.

• Seventeen individuals and one corporation have been indicted on charges related to the global trafficking of stolen credit card numbers, cybercrime, and identity theft. The 173 count indictment charges that the “Western Express Cybercrime Group,” operated from 2001 through 2007, realized millions in profits from the sale and fraudulent use of personal data. The group operated through a structure of “vendors,” “buyers,” “cybercrime service providers,” and “money movers.” The vendors sold large volumes of stolen credit card numbers and other personal information through the internet, while the buyers used the internet to purchase that information in order to commit other crimes such as identity theft. The cybercrime service providers aided and facilitated in these purchases, and other defendants acted as money movers. These individuals provided financial services and conducted transactions in order to move funds and launder the criminal proceeds; this level relied heavily on anonymous digital currencies such as Egold and Webmoney. Some individuals played more than one of these roles. In a four year period, over $35 million flowed through numerous Western Express bank accounts, and this group is responsible for over $4 million in worth of identified credit card fraud, trafficking over 95,000 stolen credit card numbers.

• A Philadelphia couple, Edward K. Anderton and Jocelyn Kirsch, have been charged with aggravated identity theft, access device fraud, bank fraud, and money laundering. According to information the couple stole purses that were left unattended at a Philadelphia bar and used the victims’ credit cards to make purchases on several occasions. The couple also stole credit card information from friends and co-workers; on at least one occasion, Anderton stole information from an application that had been submitted to his employer. On other occasions, the defendants would telephone victims and pose as either law enforcement or human resource managers, seeking more information. Over the course of one year, the couple used the identities of more than 16 victims to obtain over $100,000 in cash and merchandise, with attempts to obtain at least $112,000 in additional cash and merchandise. If convicted on all charges, each defendant faces a maximum sentence of 69 years in prison.

The Response/Current Efforts

Merchants are more at risk from credit card fraud than are consumers. Regardless of whether the transaction occurred in person or on-line, the consumer generally only has to face the hassles of reversing a fraudulent charge, canceling their lost or stolen card, or paying the first $50 of the loss (although most credit card companies waive this fee). In contrast, a merchant loses the cost of the product sold, must pay numerous credit card charge-back fees, and even faces the possibility of having their merchant account closed.

Many methods of safeguarding credit card purchases exist. Credit card companies started using holograms in 1981 to identify genuine cards at the time of purchase. At the same time, large-scale hologram counterfeiting operations developed in Taiwan, Hong Kong, and China. A separate market emerged for these holograms, which sell for between $5 and $15, depending on the quality of the hologram. In 1994, the Canadian Combined Forces Special Enforcement Unit and the Combined Forces Asian Investigation Unit
arrested members of a Chinese syndicate that produced approximately 300,000 counterfeit holograms and had distributed 250,000 of them. Based on the quantity delivered and using an estimate of $3,000 lost per card, Visa and MasterCard estimated that their combined losses caused by this group approached $750 million.\(^{19}\)

The FTC recommends that consumers sign their cards in a manner that requires the user to show photo identification, carry their cards in a separate compartment of their wallet or purse, destroy carbon copies, void incorrect receipts, reconcile monthly account statements, and shred unsolicited credit card offers.\(^{20}\) These steps will reduce the likelihood of either fraudulent purchases charged to the victims' accounts or more severe identity theft.

Credit card fraud is a recognized issue of import. One problem facing the struggle to reduce this type of fraud, however, is the lack of law enforcement resources devoted to this type of crime. Although law enforcement acknowledges the extent of the crime, resources are often such that many agencies are simply not able to allocate the time and manpower needed to police these crimes. This is especially true when a fraudulent transaction may only account for $20-50 loss per victim, such as with the recent cases involving the company Pluto Data.\(^{21}\) While these fraudulent transactions are noteworthy, they may simply not garner the resources that more salient crimes attract. Additionally, many credit card frauds may suffer from jurisdictional problems; for instance, many of the fraudulent transactions may take place in a city, state, or country other than that in which the victim is residing. Due to the lack of consistent law enforcement involvement and jurisdictional issues, ensuring transaction safety often falls to the individual; as a consequence, many, especially merchants involved with online transactions, utilize a variety of methods for ensuring credit card security and safety.

Internet credit card transactions are referred to as CNP (cardholder not present transactions). In order to validate a card, many on-line merchants use cardholder recognition software, validity checks, and red flag order settings. These “red flags” are based on subtle differences in the card’s information that have also proved fraudulent in past purchases. For example, one red flag arises when the shipping and billing addresses are not the same. This is especially true in situations involving PO Boxes and private, rented boxes (e.g., at Mailboxes Etc.). Other types of red flags are purchases of high dollar items or orders in multiples with requests for rush or expedited shipping. On-line criminals generally like to receive their items quickly for resale purposes and, since they have no intention of paying the bill, they do not mind the higher cost for shipping.

One of the latest technological advancements in the race to foil credit card fraudsters is the employment of new chip-based technology in credit cards. Rather than relying on the standard magnetic strip to divulge card owners’ information, the new technology stores this information on a computer chip embedded within the card which requires a pin to unlock—a practice that is currently underway in Europe and has been going on in France for over ten years, where credit card fraud has dropped 80%.\(^{22}\) This system is currently being unveiled in Canada and is also being employed by select card issuers in the U.S.

Also, both Visa U.S.A. and MasterCard currently offer state-of-the-art identity check offerings. Visa U.S.A. invited cardholders to link their cards to passwords that would be required when shopping at participating on-line stores. The service, “Verified by Visa,” is designed to raise the level of security and allay fears of fraud that haunt many merchants and consumers. Verified by Visa is a way to authenticate on-line buyers to on-line sellers in which customers register for a password with the bank that issues their credit card. Merchants are linked back to the card issuer that verifies the cardholder's identity based on that password. In addition to programs such as “Verified by Visa”, Visa is also using a new “advanced authorization” system.\(^{23}\) By evaluating 40 variable factors (such as whether or not the card being used was part of a known security breach or if items are being ordered at a high-volume quick rate), the system can provide banks with an instant rating of the transaction's potential for fraud, allowing the issuer to decline the purchase if warranted. This new system is reported to be able to flag up to 40% of false transactions which may have gone undetected previously.

Additionally, many major credit card companies have banded together to help to ensure safety by issuing what is known as the Payment Card Industry Data Security Standard (PCI DSS). This standard requires all merchants to follow the same guidelines of data security. It is unknown how many retailers are PCI
compliant, but Visa estimates that upwards of two-thirds of its large and medium-sized merchants meet requirements as of January 2008. In order to assist business owners in this endeavor, card companies and payment processors are supplying tutorials and Webinars to business owners in order to help navigate the intricate technology regulations. The latest version of the security standard is scheduled for release in October 2008.\textsuperscript{24}

Recent initiatives in an effort to battle credit card fraud and identity theft have also emerged on a federal level. A recent amendment to the Fair Credit Reporting Act requires consumer reporting companies to provide consumers with a free copy of their credit report (including information on where you live, how you pay your bills, and whether you’ve been sued, arrested, or filed for bankruptcy) once every 12 months, at the consumer’s request. This went into effect on December 1, 2004 in the Western states and is now available nationwide.\textsuperscript{25} This allows consumers the ability to closely monitor their own credit histories without paying charges to reporting agencies.

\textbf{“For More Information” Links}

- National Check Fraud Center – www.ckfraud.org

\textit{Maintenance and revisions:} April D. Wall, NW3C Research Associate

© 2008. National White Collar Crime Center. All rights reserved. The National White Collar Crime Center (NW3C) is the copyright owner of this white paper. This information may not be used or reproduced in any form without the express written permission of the NW3C.
Endnotes


