DISCUSSION PAPER
PAYMENT CARDS CENTER

Fraud Management in the Credit Card Industry[1]

Peter Burns
Anne Stanley

April 2002

Summary*: On November 16, 2001, the Payment Cards Center of the Federal Reserve Bank of Philadelphia sponsored a workshop on fraud management in the credit card industry. Daniel Buttafogo and Larry Drexler of Juniper Bank led the discussion.[2] Daniel Buttafogo, Director–Risk Management, is Juniper's fraud expert. He provided an overview of fraud in the card industry and discussed some of the challenges he faces as a risk manager. Larry Drexler is General Counsel and the Chief Privacy Officer at Juniper. Following Buttafogo's remarks, he led a more general discussion on how fraud protection and security can be placed in the context of the broader public policy debate on information privacy. This paper summarizes these two executives' presentations and is supplemented by additional research.*

[1]The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.
[2]Juniper is an Internet based credit card company established in October 2000. Based on an innovative business model and web site, the company's November 2001 receivables had grown to approximately $350 million with more than 185,000 accounts. In October 2001, Canada's Canadian Imperial Bank of Commerce announced an equity investment in Juniper leading to a 51% ownership position.

FEDERAL RESERVE BANK OF PHILADELPHIA
Ten Independence Mall, Philadelphia, PA 19106-1574• (215) 574-7220• www.phil.frb.org

DEFINING CREDIT CARD FRAUD

Buttafogo began the workshop with a working definition of credit card fraud as: "Unauthorized account activity by a person for which the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future." He then described the range of fraudulent activities observed in the industry.

Application fraud. Application fraud can take two forms, "familiar" and "unfamiliar." The "familiar" version occurs when a family member, roommate or personal acquaintance with easy access to an individual's mail and personal information (i.e., social security number, date of birth, etc.) fills out a credit card application sent to the individual and then upon receiving the card, uses it as if he were the true cardholder. Once identified, these situations are generally resolved by the individuals involved. The fraudulent party is well known to the victim and restitution is often made to avoid embarrassment to the family or friends. Application fraud from an "unfamiliar" source occurs when a person unknown to the victim gains personal information about the victim, obtains a card in the individual's name and proceeds to use it without the individual's knowledge. Personal information used in the fraudulent application is secured using a variety of illegal tactics, often aided by technology. Internet search engines and databases have made it far easier to obtain social security numbers and other personal information used in the card application process. This is a form of

identity theft that often results in serious difficulties for the victim once the fraud has been identified and the individual works to re-establish their credit record.

Lost and stolen credit cards. According to Buttafogo fraudulent use of lost or stolen credit cards is the most common form of abuse in the industry. When a credit card is lost or stolen the criminal gains direct access to the individual's credit card account. The criminal may also gain access to other personal information about the individual as the lost and stolen credit cards are often contained in wallets, purses and briefcases. This may compound problems if the information is used to broaden the fraud, for example by applying for other cards. Fortunately, most lost or stolen cards are quickly recognized and upon notification of the issuer, losses can generally be minimized. More importantly for consumers, card issuers generally indemnify their customers from fraudulent use if the theft or loss is promptly reported.

Non-receipt (mail intercept) fraud. Non-receipt or mail fraud occurs when an individual's mail is intercepted by a criminal. Most issuers have card activation programs requiring customers to call and authenticate in order to begin purchasing with their card. These programs help mitigate non-receipt losses and enable issuers to quickly detect non-receipt fraud.

Counterfeit cards. A counterfeit card is created when a criminal gains possession of a valid card number. This information can then be encoded on a

blank card's magnetic stripe or manually changed on the face of a stolen plastic. A quick search on the Internet can provide the criminal with all the resources to manufacture fraudulent cards. Custom embossing machines, tipping machines, decoding machines, programs for encoding credit card magnetic stripes, and various other tools for the production of counterfeit credit cards are all available from a variety of Internet sites.

Prior to the introduction of real time terminal authorizations, criminals were able to create false cards simply by obtaining card information from discarded sales receipts. In today's electronic world, additional information contained on the card's magnetic stripe is read by the authorization terminal. Simple hand held devices are now available to criminals that can be used to "skim" the magnetic stripe and obtain all the information needed for the creation of a fraudulent card. Virtually all merchant terminals employ this technology in the form of an electronic card reader. These devices serve the legitimate purpose of capturing the information which is encoded in the magnetic stripe on the back of credit and debit cards, including such authentication data as the cardholder's name, account number, issuing bank identifier, etc used to authorize a transaction. When skimming is used with criminal intent, this same information can be used directly over the telephone or Internet for unauthorized purchases or as the basis for producing counterfeit cards. Initially, skimming devices were connected to the phone line between the phone jack and the credit authorization terminal. When a credit card purchase is made, the card is swiped for authorization, and the electronic skimmer captures the information and stores it for later use. Unless the

merchant is involved in the fraud, these devices are relatively easy to identify and disable.

In recent years, the industry has witnessed significant growth in this abusive practice with the development of small, portable devices which can store up to 100 account numbers at a time. Once in possession of a customer's credit card, the criminal can run the card through this easily concealed device and in seconds access and store the magnetic stripe information. Skimming usually occurs in businesses where the normal transaction requires the cardholder to give up possession of the card, such as in a restaurant.

Manual counterfeit occurs when a valid account number is stolen or is created using card number generation software and then manually embossed on the front of a blank card. The perpetrator will then erase any data stored on the magnetic stripe of the blank card and present it to a merchant for a purchase. Since the magnetic stripe is not readable, the merchant is forced to manually enter the number off the front of the card into the POS terminal. This allows the criminal to evade many of the issuer's authentication systems.

Account takeover. Account takeover occurs when a criminal obtains enough personal information about an individual to effectively represent the person with the card issuing bank. The first step in the criminal process is to request a change of address on the account. A subsequent call to report the card lost or stolen leads to a new card being mailed to the changed address. The criminal has now successfully taken over the account – hence the term "account takeover." To

combat this abuse, the three credit bureaus and issuing banks make it common practice to verify by phone and/or duplicate mailings to both addresses any such change of address requests.

CARD-NOT-PRESENT TRANSACTIONS

In general, the fraud tactics described above relate to the world of physical cards. Credit card use where the physical card is not present at the point of sale (POS) creates a different set of challenges. Within the payment cards industry this is referred to as the mail order/telephone order (MOTO) arena. MOTO transactions are card-not-present transactions and include the use of credit cards on the Internet. These transactions all share the fundamental problem of authentication, the ability to verify that the purchaser is actually the cardholder. The mail order and telephone order environment offers at least some level of authentication assurance. Most of purchases are made from directed mail of a catalogue to a specific address with a customer identification number. This information is used by the merchant to verify that the caller, (or mailer) is associated with the catalogue mailing address and customer number.

In the Internet world there is no such connection. The order flows anonymously from a computer that can be located anywhere with no ability for the merchant to authenticate that the card number presented is associated with the actual cardholder. At this point there is no authentication system that has been generally adopted by all parties (credit card associations, issuers, merchants and consumers). Smart cards used with readers attached to computers offer one possible solution; but to date there has been little interest by consumers or computer manufacturers to invest in this technology. Issuers broadly indemnify cardholders from Internet fraud; therefore there is little incentive for

consumers to make such investments. Association rules allow issuers to charge back these fraudulent transactions to merchants, which further diffuses incentives to tackle the problem.

Another factor, according to Buttafogo, is the percentage of Internet fraud transactions that may be classified as "familiar fraud." A transaction may be legitimately initiated by the cardholder for a product that could be considered dubious in nature, (i.e., pornography on the Internet). When confronted by a family member the individual may deny knowledge of the transaction and then report it as fraud. A legitimately billed transaction can then be reported as "never received" and reversed by the issuing bank. The *U.S. Banker* in a December 2001 report on cyber-fraud entitled, 'I Didn't Do It' suggested that pornography charges like these probably accounted for half of all online fraud.

Buttafogo then spoke about an even more insidious abuse in the card not present Internet environment. Computer programs, such as CreditMaster and Credit Wizard, are easily available on the Internet, and can be used to generate sequences of 16-digit credit card numbers from valid Bank Identification Numbers or BINs (the first six digits of any card number). This enables the criminal to quickly transact multiple fraudulent sales from online merchants whose security does not block sales to sequential numbers. According to Buttafogo, these programs are the favored tools of organized gangs who are believed to be responsible for a significant percentage of the dollar losses associated with Internet fraud.

DETECTION & FRAUD RISK MANAGEMENT

Buttafogo described and explained industry detection and risk management practices. Detection and prevention of fraud is an extremely important form of risk management in the credit card industry. According to a May 2001 bankcard profitability study from *Credit Card Management*, the industry loses close to one billion dollars a year from fraud. These are losses to the card issuing companies and do not include the fraudulent transactions charged back to merchants in the MOTO environment described above.

Application process. The application process represents the first line of risk management defense. It is common practice for card issuers to confirm an applicant's information through multiple data sources. Many issuers may also do phone address/distance calculations to determine if the phone number on the application matches the address as defined by the area code on the application. Certain high-risk applications may be pulled for a detailed review depending upon the channel used, the applicant's geographic location or other special characteristics. Unsolicited applications from the Internet channel are almost always reviewed given the authentication problems described above. Applications may also be pulled for review when received from geographic areas where high incidences of credit card fraud have been reported in the past. Applications are also tested for inconsistencies with information received from credit bureaus. These might typically include names, addresses or phone numbers that do not match and might signal an attempt to create a fraudulent account.

Activation process. Issuers also build in fraud controls when a new card is activated by the customer. When calling to activate the card a flag may be raised if the call does not originate from the home phone number listed on the application. In such circumstances, rather than automatically activating the account, the caller is transferred to a customer service representative who will attempt to verify the caller's identity using other information from the application or information obtained from the credit bureaus.

Transaction behavior monitoring. Sophisticated card issuers monitor high-risk situations and transactions in a proactive attempt to prevent fraudulent transactions. Examples of high-risk situations that may receive special monitoring would include the opening of new accounts and the sudden and intense usage of cash advances. Sophisticated neural network software is commonly used to monitor transaction behavior to flag unusual activity. For example, a series of cash advances by a cardholder who rarely uses his card for cash advances may trigger an investigation and perhaps a call to the cardholder to verify these cash transactions. Similarly, large dollar purchases at a location far removed from the cardholder's normal purchasing area might similarly be flagged for further investigation and verification. All such high-risk activity and transactions are typically reviewed against files of known lost or stolen cards.

Fraud control at the point of sale. While issuers rely on information management technologies to identify potential cases of fraud, merchants at the point of sale may physically identify a card that appears altered or encounter situations where a customer's identity may be questioned. Merchants, however, are often in a difficult position. The cost of wrongly accusing a customer of fraudulent behavior is high. As such, strategies at the point of sale must balance the desire to avoid fraudulent transactions while managing positive customer relations. Merchants, with the issuer's approval, will often authorize a suspicious transaction for a moderate amount. This is to avoid the risk of offending what might be a legitimate customer. Declining the charge offers an anonymous way to avoid confrontation and is often employed for suspicious larger dollar transactions. The merchant simply tells the customer that the charge cannot be authorized by the issuing bank. A customer can also be asked to call the card issuer at the point of sale to verify their identity over the phone. As a last resort, the merchant can physically seize the card in an obvious case of fraud. However, given the potential for volatile confrontation this rarely occurs.

DETECTION & FRAUD PREVENTION ON THE INTERNET

As described earlier, the Internet and the anonymity associated with card not present transactions present unique fraud management challenges. Authentication of the cardholder is a fundamental requirement in managing fraud on the Internet and there are no universally accepted solutions. As a result, credit card fraud on the Internet is substantially greater than in the physical, or even, phone environments.

One approach to combat Internet fraud, which is supported by many issuers, is Card Verification Value 2 (CVV2). The set of three digits found on the reverse side of most credit cards is unique to that card. Merchants that require Internet customers to enter this value along with the actual card number, add a layer of security to the transaction. Since the three-digit value can only be found on the card itself, there is a greater likelihood that the purchaser is actually in possession of the card. Stolen charge receipts, for example, would not reveal the card's three-digit card verification value. However, if the card being used has been stolen, this is obviously not an effective preventive measure.

The use of account number masking software is another new method being employed as a way to control Internet fraud. The key element of this process is a single use number for each transaction. A handful of issuers have unveiled programs that add this extra step to the online shopping process. Generally, after the consumer has selected their items for purchase from an e-tailer and is ready to "check out," they then log on to their card issuer's web site. On the web site they select the card they wish to use to pay for the purchase. At this point a unique credit card number and expiration date is created and used to finish the online purchase. To date, these single use number programs have not been widely accepted and utilized. Anecdotally, it has been suggested that consumers are unwilling to accept the inconvenience associated with the added steps. Other observers suggest that consumers simply are not that concerned about using credit cards on the Internet.

An important underlying factor in the dealing with fraud on the Internet is that, as previously noted, merchants, rather than issuing banks or consumers are responsible for most of the financial cost of card-not-present fraud. Therefore, there is no strong coalition

among the other players involved to find a solution to beat card-not-present fraud. Merchants, who have the largest incentive to participate in programs, are not likely to invest the time and money required for implementation until there is a agreement on a specific program by all the parties involved (credit card organizations, issuers, merchant and consumers).

BUST-OUT-FRAUD

Buttafogo concluded his section of the workshop by describing a relatively new form of credit card fraud with often very large loss consequences. "Bust-out-fraud" as defined by Buttafogo, occurs with true customers gradually building up as much available credit as possible on multiple credit cards and then "busting-out" with a rash of large cash advances, high dollar value convenience checks, or purchases of easily sold merchandise such as jewelry and electronics. The perpetrator of the fraud will typically draw bad checks on one account to repay another issuer and thus re-establish credit line access. This leads to transacting more cash advances and then for all intents and purposes the perpetrator vanishes.

The difficulty in detecting this phenomenon is that until the "bust-out," these criminals exhibit behavior common to most legitimate card users, use their cards within limits and promptly pay balances when due. The consequences to issuers can be severe. Buttafogo noted that industry sources report that one credit bureau documented a collective loss of $750,000 suffered by multiple issuers from one individual. Single account losses will generally exceed credit limits by at least several times due to the "kiting" of payments among multiple issuers.

Despite the difficulty in separating these customers from the general base of legitimate customers, Buttafogo described observable activities that generally occur when these individuals decide to "bust out." They suddenly become heavy drawers of cash from their cards, quickly consume all of their credit lines and bureaus report a rash of credit inquiries as they make multiple payments within days of each other that get returned for insufficient funds. As issuers observe these behaviors most will quickly close the account. Ironically, Buttafogo reports that these criminals will often loudly complain based on their model behavior up to this point in the hope that the bank will relent and allow them to continue for even a few more days.

Buttafogo concluded with the following statement regarding his role in managing fraud control efforts at Juniper that broadly characterizes this risk management role in the industry, "My objective is to make fraud difficult to commit, detect it quickly when it does occur, stop it as soon as possible and learn how to better protect the bank in the future."

FRAUD AND THE PUBLIC POLICY PRIVACY DEBATE

Larry Drexler, general counsel and chief privacy officer at Juniper, followed with a discussion of how credit card fraud, and especially identity theft, plays out in the policy debate on information privacy. Working with the state law enforcement officials, Drexler and his industry colleagues are attempting to forge a private-public partnership to address this issue.

In Drexler's view, existing privacy protection legislation, and most recently implementation of GLB privacy statutes, effectively address the more serious risks associated with information sharing by banks and credit card issuers. Many of the

perceived risks associated with the sale of customer lists and associated bank account numbers have been addressed by legislation and regulators. Account numbers may no longer be shared with third party marketing partners and opt-out provisions provide further opportunities for consumers to control dissemination of their private personal information.

Nevertheless, Drexler anticipates that the public debate and resulting tension between the industry and policymakers on information sharing will continue. Moreover, political pressures for greater protections remain and the industry will continue to be challenged to demonstrate the value consumers derive from responsible industry information sharing practices.

In the interim, Drexler argues that the industry and policymakers may be better served by identifying areas to work together where common interests are clearer. Insuring the security of customers' personal information may well be one area where agreement can readily be reached. Credit card fraud adds additional costs to the industry which are ultimately passed on to cardholders and consumers in the form of higher prices. While consumers are generally indemnified for direct losses arising from credit card fraud, the costs to victims of identity theft can be substantial. The time and expense associated with restoring one's credit standing is only part of the cost incurred by the victim. For many, the emotional cost of this highly personal invasion of privacy is the more damaging outcome. As such, Drexler believes that a coordinated assault on credit card fraud, and particularly identity theft, effectively joins the public and industry's interest.

With this in mind, what can de done? To date the payments card industry and relevant government agencies have been addressing the issue from largely independent positions. Drexler believes that a coordinated private-public partnership can greatly leverage these independent initiatives. He notes three specific areas where partnerships can be a more effective tool than independent action:

Aggressive prosecution of perpetrators of fraud. The experience of industry professionals suggests that many of the perpetrators of credit card fraud are repeat offenders who have not been deterred by limited legal consequences. The industry understands the various criminal schemes employed and law enforcement agencies have the means to pursue and prosecute offenders.

A pro-active approach to assist the victims of identity theft. Working together, account holder banks, credit bureaus, legislatures, and law enforcement agencies can greatly facilitate and streamline the current burdensome process of restoring a victim's credit standing.

A coordinated approach to consumer education. Industry research suggests that many victims of credit card fraud were unaware of the dangers associated with indiscriminate disclosure of account numbers and other related risky behavior. Again, the industry understands these risks and public sector agencies have the ability to provide appropriate educational support to the broad base of consumers.

In pursing the development of a private-public partnership to address these issues, Drexler and industry colleagues have begun a dialogue with state law enforcement officials. These officials are well positioned to lead on the prosecution front and could provide support for broader protection efforts that might be a result from a cooperative dialogue with the industry.