CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Research Papers in Economics

payments system research briefing

MAY 2006

FEDERAL RESERVE BANK of KANSAS CITY

Payments Fraud: Consumer Considerations

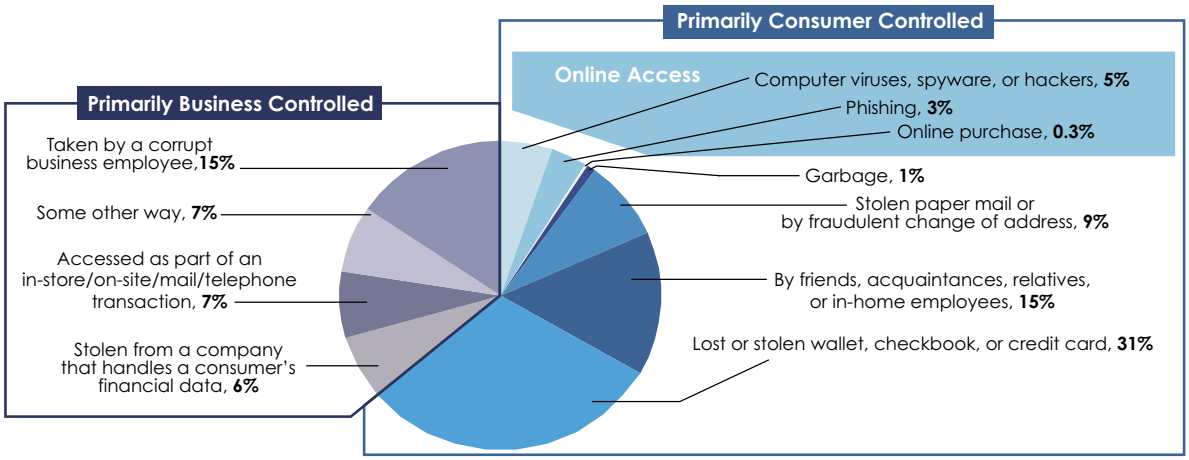
by Terri Bradford, Payments System Research Specialist, Federal Reserve Bank of Kansas City, and Bruce Cundiff, Research Analyst, Javelin Strategy & Research

How to pay? This is a question consumers are confronted with every day. Should you use cash, write a check, authorize a debit to your checking account by phone or online, use a credit or a debit card? And for debit card transactions, should you sign or enter a personal identification number (PIN)? With each method of payment, your perception of the risk of fraud might enter into the decision.

Payments fraud—the use of a payment mechanism by someone other than the individual(s) authorized to use it—has become more and more common. As illustrated in Chart 1, fraud is most often conducted in very "low-tech" ways, for example, from simply misplacing a purse or wallet as compared to more sophisticated scams like skimming or phishing. While payments fraud affects businesses and consumers alike, this *Briefing* article examines the potential for fraud associated with various "traditional" payment methods and the protective measures that consumers should take when using them.

Chart 1

How Fraudulently Used Consumer Information is Obtained



Note: The sample size was 206 respondents. The base was those who knew how their information was obtained.

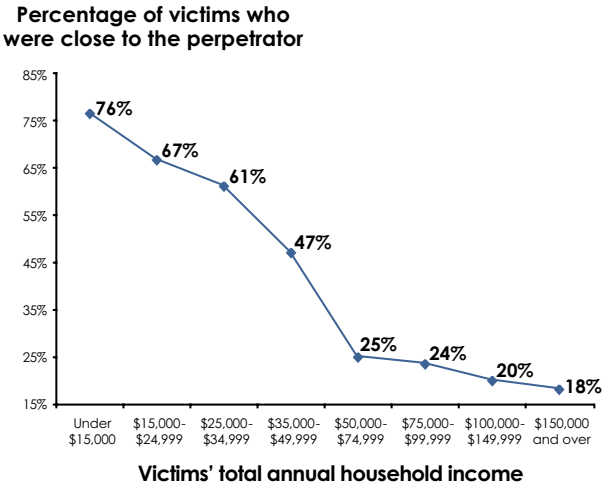
© 2006 Javelin Strategy & Research

General considerations

As illustrated in Chart 2, Javelin Strategy & Research data indicates that a relatively high percentage of fraud victims personally knew the perpetrator, as he or she was either a friend, relative, or in-home employee. This is especially true for fraud victims with less than $50,000 in annual household income. Such occurrences highlight the need for consumers to safeguard information not only at the point of transaction, but also in the home.

Chart 2

Percentage of Fraud Perpetrated by People Close to the Victim
(By income)



Note: The sample size was 182 respondents.

© 2006 Javelin Strategy & Research

The precautionary measures consumers should take with each payment mechanism to combat fraud should take into consideration both the sources of fraud and the ease of resolution based on the payment type. With checks, a debit authorized via the Internet or phone, or debit card payments, it is important to note that the consumer is providing access to his or her demand deposit account (DDA) at his or her financial institution. Should fraud occur, the impact at a minimum will be the unplanned loss of funds, which could ultimately result in legitimate payments being returned because of insufficient funds in the consumer's account. Consequently, the consumer also may be hit with insufficient funds fees.

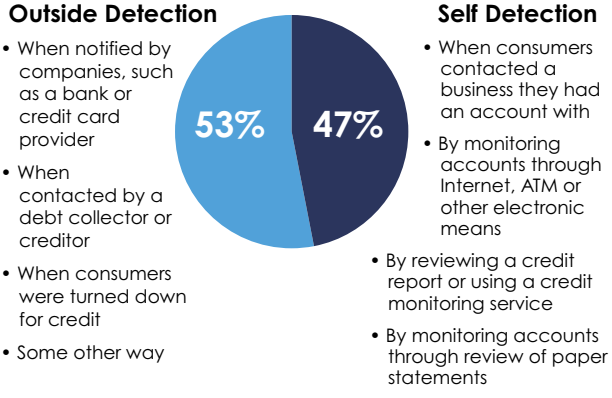
While losses may be capped according to established regulations or laws, consumers must be vigilant in monitoring their accounts and promptly notifying their financial institutions. For example, the Uniform Commercial Code dictates that consumers have responsibility for discovering and reporting unauthorized signatures or alterations to their checks with a reasonable promptness (typically defined by financial institutions as 30 to 60 days). For unauthorized ACH debits initiated either online or by phone, the National Automated Clearinghouse Association (NACHA) dictates that consumers must notify their financial institution within 15 calendar days of receiving notification of the debit from their financial institution (this typically occurs via a bank statement). Finally, as it relates to card fraud, the card networks' rules govern notification requirements, but typically the consumer is protected by zero liability coverage.

Fraud detection

Detection of fraud typically occurs in two ways: either another party provides some form of notification to the consumer or the consumer discovers the fraud through some due diligence of his or her own. As illustrated in Chart 3, Javelin data indicate that nearly half of all identity fraud is detected by the consumer.

Chart 3

How Identity Fraud is Detected



Note: The sample size was 466 respondents. The base was those who knew how identity fraud was detected.

© 2006 Javelin Strategy & Research

Consumers, therefore, have a clear role to play in protecting themselves from fraud when using different payment methods and also in detecting potentially fraudulent activity.

Paper checks

Paper checks are a declining payment choice, but old habits are hard to break, and consumers certainly will continue to write them. Every time a personal check is used, the consumer is handing over a wealth of information to a surprisingly large number of people who must handle the check in order to complete the payment clearing process. Included on a check are the consumer's name, address, phone number, checking account number, and bank location at a minimum. Additionally, a driver's license and social security number (SSN) may be included, although this practice is decreasing. Now, consider the number of people who handle a paper check after it is written—the store clerk who places it in a register drawer; the manager who makes the bank deposit; the bank personnel and staff who work at other financial institutions; and transportation companies involved in the paper check clearing process.

Any of these people could use that opportunity to commit either new account fraud, which is the use of sensitive personal information to open new accounts in the consumer's name, or existing account fraud, using the account to initiate fraudulent transactions. Javelin Strategy & Research data indicate that 15 percent of all identity fraud—roughly $8.5 billion—is a result of information taken by a corrupt business employee,[1] as described in the previous example. The "low-tech" nature of the majority of payment fraud, in addition to the sizeable percentage of fraud perpetrated by those who are known to the victim, makes the proper storage, protection, and use of paper checks of paramount importance.

Actions that consumers should take to protect themselves from fraud include, but are not limited to:

- Keeping checks locked and safe at home;
- Ensuring that when mailing checks, all mail is placed in a locked mailbox, or even taken to the post office;
- Allowing merchants to convert the check to an electronic transaction when possible, or paying bills online;
- Having some level of trust of the merchant or recipient when using checks for purchases at a point of sale;
- Monitoring DDA activity to detect potential existing account fraud;
- Monitoring credit reports to detect potential new account fraud; and
- Carefully reviewing check images or copies to ensure that amounts and payee information have not been altered.

Automated clearinghouse transactions

While safer than paper checks in terms of the amount of information available for fraudsters and the number of times the information is handled, automated clearinghouse (ACH) transactions still have inherent risks because, just like paper checks, they provide a source of access to consumer DDAs. In order to effect an ACH payment, consumers must first provide a third party with their bank routing transit number and checking or savings account number. In the hands of the wrong individuals, the result could be unauthorized debits to their accounts.

Actions that consumers should take to protect themselves include, but are not limited to:

- Having a level of trust and some base knowledge of the individual/entity to whom/which they are providing their bank and account information;
- Closely monitoring account activity; and
- Protecting account information by not leaving documents containing that information unprotected.

Debit card payments

Debit cards provide consumers with speed and convenience but, like checks and ACH payments, access their checking account. Many consumers prefer using debit cards over credit cards because they can manage their finances more closely, spending only available funds. As a result, the fraud implications associated with debit cards are similar to paper check and ACH transactions, but many issuers have applied the same zero liability protections that are afforded to credit card users. Debit card users also have the option of authorizing transactions with either a signature or by entering a PIN. Until recently, PIN debit was thought to be the more secure authorization option, given that it involved authentication. However, recent well-publicized PIN-debit fraud schemes have been discovered. Actions consumers should take to minimize exposure to fraudulent signature-debit transactions mirror those that should be taken with credit

as discussed in the following section. Additionally, when it comes to protecting their PINs when using PIN-debit cards:

- Consumers should be alert and guard against preying eyes or hidden cameras, and protect the number so that it never becomes known to others; and
- The PIN should never be recorded on the card, carried with the card, or left in an unprotected location.

Credit card payments

Making payments by credit card well may be one of the safest options when it comes to fraud concerns. Credit cards, on their surface, do not contain any personal information other than the cardholder's name, which by itself is an unlikely source of new account fraud. Additionally, the consumer has an opportunity, in most instances, to maintain physical control of the card. If a fraudulent transaction should occur, the consumer is protected by zero liability policies that make the existing account fraud levels less burdensome. Nonetheless, credit card fraud is a significant issue and at the very least a hassle for consumers. Cardholders should be wary of the following:

- Skimming, which can occur when a card is swiped and the magnetic stripe information gathered, enabling the replication of the card to perpetrate fraudulent transactions—this is of particular concern in restaurants where the card is often out of the cardholder's control for some time;
- Theft of the physical card, which can occur at the mailbox, or when a purse or wallet is misplaced or stolen (This is still the primary source of existing card fraud.); and
- Online usage, which while resulting in relatively little technical threat that card information will be stolen online, can result in theft via social engineering—a fraudster deceiving the consumer into providing account and other personal information (access passwords, SSN, etc.).

Actions consumers should take to protect themselves include, but are not limited to:

- To the extent possible, maintaining control of the card at all times;
- Eliminating paper statements to avoid theft of information from the mail;
- Constantly monitoring accounts (online if possible), as card fraud is frequently detected by cardholders and more frequent monitoring leads to earlier detection of potential fraud;
- Having all phone numbers handy to call credit card issuers in the case of suspected fraud or a lost card; and
- Having some level of trust with online merchants where the card is used. Never provide card information online via e-mail or enter it at a site you don't trust. Look for the "lock" when entering information, which is an indication that the site is secure.

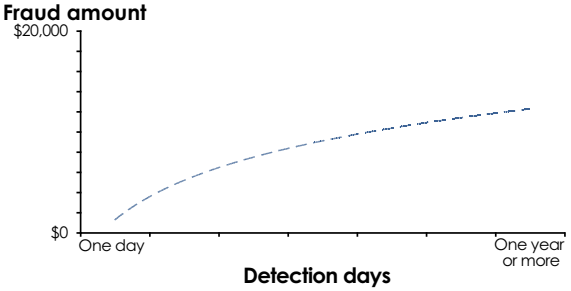
When prevention fails…

It also should be noted that in addition to existing account fraud, fraudsters can open new credit accounts in consumers' names if they obtain the sensitive personal information mentioned above. New accounts fraud is much more difficult to detect, often results in much larger fraud amounts, and is much more burdensome for consumers to resolve. Consumers can successfully guard against new accounts fraud by regularly monitoring their credit reports for activity or accounts that are not immediately recognized. Chart 4 illustrates the impact that quick detection can have on the dollar value of fraudulent card activity.

Consumers must understand that their own education and interaction with their financial institutions contribute greatly to the mitigation of fraud. There are concerted efforts and actions consumers can take on their own and with their banks to reduce the probability of becoming fraud victims—either through the various methods of payment they use or through the protection of their personal information. However, should fraud occur, more timely consumer detection of fraud naturally leads to a less burdensome experience for consumers and also potentially can lower out-of-pocket losses. Detection methods vary among payment types, but frequent and meticulous monitoring of accounts, and even credit reports—particularly through the online channel—has been found to be a primary way for consumers to detect and abate fraud.

Chart 4

How Length of Time for Fraud Detection Impacts Fraud Amount



© 2006 Javelin Strategy & Research

Endnote

[1]Javelin Strategy & Research 2006 Identity Fraud Survey Report, January 2006.

payments system research

Web site: *www.KansasCityFed.org/home/subwebs.cfm?subweb=9*

The Payments System Research Department of the Federal Reserve Bank of Kansas City is responsible for monitoring and analyzing payments system developments. Staff includes:

Terri Bradford
Payments System Research Specialist
Terri.R.Bradford@kc.frb.org
816-881-2001

Fumiko Hayashi
Senior Economist
Fumiko.Hayashi@kc.frb.org
816-881-6851

Zhu Wang
Economist
Zhu.Wang@kc.frb.org
816-881-4742

Nathan Halmrast
Research Associate
Nathan.Halmrast@kc.frb.org
816-881-4721

Rick Sullivan
Senior Economist
Rick.J.Sullivan@kc.frb.org
816-881-2372

Stuart E. Weiner
Vice President and Director
Stuart.E.Weiner@kc.frb.org
816-881-2201

The views expressed in this newsletter are those of the authors and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or the Federal Reserve System.