



Taken to Lunch

After grabbing lunch at a fast-food restaurant one afternoon, Jason Snyder ended up with a tab totaling more than \$10,000—and a lot of frustration.

As Jason Snyder unsuspectingly filled out a check to pay for his meal, he chatted with the cashier, who asked if Snyder worked in that area of Oklahoma City, or attended the university nearby.

“I just thought he was being friendly,” Snyder recalled. “I didn’t think anything of it.”

It wasn’t until more than a year later when Snyder was rejected for a car loan that he realized the cashier used not only personal information printed on the check, but also details

from that casual conversation to get a student loan at a local college.

The then-20-year-old had a harsh realization: “I had uncollected debt and bad credit.”

Snyder, who rarely wrote checks and does so even less frequently now, still may have been victimized even if he had opted for a different payment method.

“With any form of payment there is a risk,” says Terri Bradford, Payments System Research Specialist with the Federal Reserve Bank of Kansas City.

Bradford and Bruce Cundiff, an analyst for Javelin Strategy & Research, recently collaborated on a summary of the firm's study on how payments fraud—the use of a payment mechanism by someone other than the authorized user—is becoming more common. The study's findings indicate fraud is most often conducted in low-tech ways, compared to more sophisticated scams that may rely on technology.

While risk exists, Bradford and Cundiff say there are equally easy ways for consumers to prevent or reduce payments fraud, taking into consideration both the sources of fraud and the ease of resolution based on the payment type.

Significant impact

Snyder is just one of the millions of fraud victims. More than 9.3 million Americans were victimized during a one-year period, according to a 2005 study sponsored by Visa USA, Wells Fargo Bank and CheckFree Services Corp.

Snyder's brief encounter with the fast-food cashier was enough for the fraudster to assume Snyder's identity on a loan application. The culprit spelled Snyder's name incorrectly, but knew enough details, such as Snyder's place of employment and financial institution, to obtain a loan.

Later, authorities told Snyder the cashier used this same strategy to take out almost \$200,000 in loans at the same school using the identity of more than 20 others.

If fraud occurs, the minimum impact will be the unplanned loss of funds, which could ultimately result in legitimate payments being returned due to insufficient funds in the account. Furthermore, the account holder may experience corresponding insufficient funds fees. Or, the impact may be more severe, as in Snyder's case, resulting in marred credit and trouble getting loans and credit cards.

Whether victimized by an online scam or having your wallet stolen, the financial and emotional effects are usually significant, says Jay Foley, co-founder of the Identity Theft Resource Center, a national nonprofit

organization that serves as a resource for fraud victims. Foley started the agency in 1999 with his wife, Linda, who was a victim of identity theft a few years earlier.

Although fraud victims can receive assistance from these types of agencies, along with law enforcement, credit bureaus, and their own financial institutions or card networks, Foley says personal and professional experience has taught him the best way to combat fraud is prevention.

"People just don't know how," he says.

Detecting fraud

Fraud is usually discovered in two ways. According to Javelin research, the consumer in most instances (53 percent of the time) is notified by another party such as a bank or credit card provider. Otherwise, it is discovered by the consumer (47 percent of the time) when monitoring accounts or credit reports, for example.

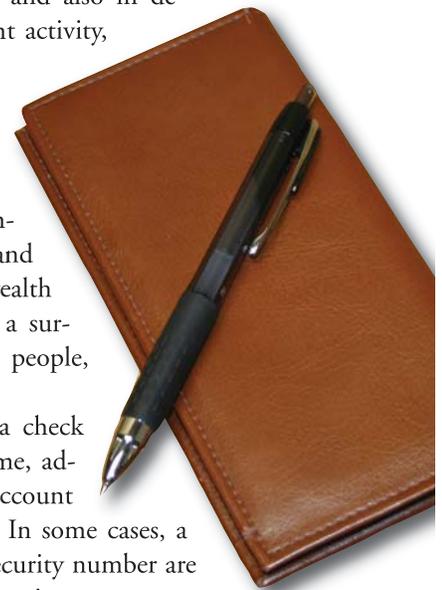
Consumers have a clear role to play in protecting themselves from fraud when using different payment methods and also in detecting potentially fraudulent activity, Bradford and Cundiff say.

Checks:

Although it is a declining payment choice, many consumers are still reaching for their checkbooks, and in turn, handing over a wealth of personal information to a surprisingly large number of people, Bradford says.

Typically included on a check are the account holder's name, address, phone number, account number and bank location. In some cases, a driver's license and Social Security number are also included, but this is becoming rare.

After a check is written, these details are then passed to everyone involved in the check clearing process: store employees, transportation staff and bank personnel. There are numerous opportunities to commit fraud by



either opening a new account or tapping into the existing account. Roughly 15 percent of identity fraud, equating to \$8.5 billion, is the result of information taken by a corrupt employee, according to Javelin research.

There are several consumer safeguards, including keeping unused checks locked up at home, mailing checks from a locked mailbox or from the post office, allowing merchants to convert checks to electronic transactions, paying bills online, patronizing trusted merchants or recipients, monitoring account activity, and reviewing cleared checks to ensure they have not been altered.

ACH transactions:

Automated clearinghouse (ACH) transactions, such as payroll direct deposit or direct payment of bills such as mortgages or loans, are a safer payment method than writing checks because both the amount of information available and the physical handling of that information is reduced. However, there is still risk because consumers must provide third parties

with account numbers.

Methods of fraud protection include monitoring account activity, securing documents, and providing account information to trusted entities or individuals.

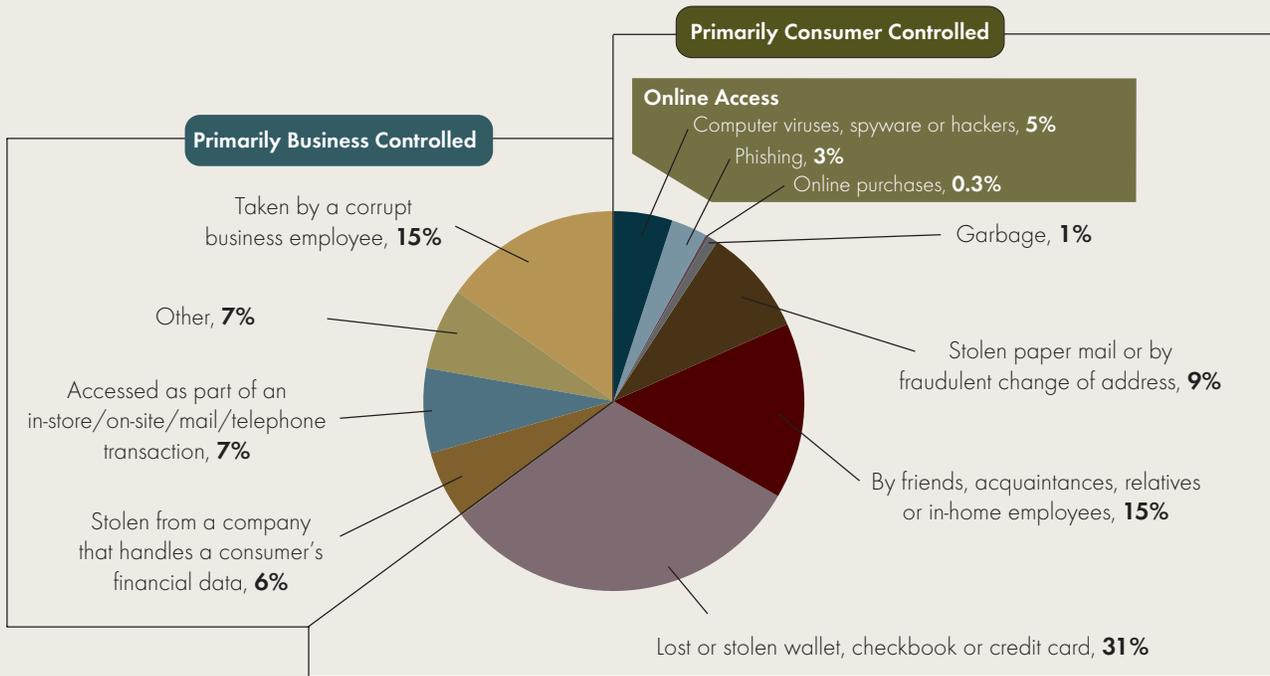
Debit and credit cards:

Like checks and ACH transactions, debit card payments also may provide unwanted access to consumers' checking accounts. The fraud implications (direct loss of funds and immediate impact) are similar as well, but many debit card issuers apply the same "zero liability" protection that credit card networks offer.

Both PIN and signature authorization for debit card use should be protected to avoid fraud. PIN users should guard themselves so others can't see the numbers entered. The PIN itself should never be written on the card or left unsecured. Securing debit cards is similar to credit card precautions.

"Credit card payment may well be one of the safest options when it comes to fraud concerns," Bradford says.

How Fraudulently Used Consumer Information Is Obtained



Note: This sample size was 206 respondents. The base was those who knew how their information was obtained. © 2006 Javelin Strategy & Research

Because credit cards physically don't list personal information other than the cardholder's name, they are an unlikely source of new account fraud. Additionally, the consumer generally maintains control of the card, as opposed to checks, which pass through many hands. If a fraudulent purchase does occur, the consumer is protected by zero-liability policies, making fraud recovery less burdensome.

monitoring their credit reports for unrecognizable activity."

Now, several years later, Jason Snyder checks his credit report every six months or so. Thankfully, there have been no other theft incidents. This steady monitoring likely would catch another I.D. thief, which is how Snyder discovered the crime. After obtaining the loans in his victims' names, the

“ Consumers must understand that their own education and interaction with their financial institutions contribute greatly to the mitigation of fraud. ”

“Nonetheless, credit card fraud is a significant issue and, at the very least, a hassle for consumers,” Bradford says, adding there are several ways cardholders can be victimized—with more methods emerging continually.

“Skimming,” for example, occurs when a card is swiped and information is gathered from its magnetic stripe, allowing replication and fraudulent charges to be made. Online credit card usage is also a threat. Although stolen card information is infrequent, fraudsters via social engineering can deceive the consumer into divulging other personal information, such as a Social Security number. However, overall theft of the actual card is the primary source of fraud.

Consumer protection includes maintaining control of the card as much as possible, eliminating paper statements to avoid mail theft, constantly monitoring accounts, having phone numbers handy to immediately report incidents and having a level of trust with online merchants.

Beware

In addition to existing account fraud, with the right information, fraudsters can open new credit accounts in consumers' names.

“New account fraud is much more difficult to detect, and often results in much larger fraud amounts and is more burdensome to resolve,” Bradford says. “Consumers can guard against new account fraud by regularly

fraudster made the first few payments to buy himself more time. It wasn't until a confused Snyder analyzed again and again his tainted credit report that he realized just what had happened.

“Consumers must understand that their own education and interaction with their financial institutions contribute greatly to the mitigation of fraud,” Bradford says. “While detection methods vary among payment types, frequent and meticulous monitoring of accounts, and even credit reports, has been found to be a primary way for consumers to detect and abate fraud.”

Snyder agrees.

“It took five, six years to get this all taken care of,” he says.

The hours spent dealing with credit bureaus, financial institutions, authorities and the loan grantors added up quickly.

“I think at this point it's fully resolved,” Snyder says. “Finally.”



BY BRYE STEEVES, SENIOR WRITER

FURTHER RESOURCES

PAYMENTS FRAUD: CONSUMER CONSIDERATIONS

By Terri Bradford and Bruce Cundiff

www.KansasCityFed.org/TEN

COMMENTS/QUESTIONS are welcome and should be sent to teneditors@kc.frb.org.