Perspectives on retail payments fraud

Steve Malphrus

Let me begin by saying that I am not here to lecture, but rather to learn. Today, I would like to talk about a couple of things. First, I would like to start with some themes that emerged from a roundtable discussion that the Federal Reserve held last year with industry leaders on emerging issues involving fraud in the retail payments system. This is important to the Federal Reserve. The outputs from the roundtable are used to direct the Federal Reserve's research and inform its work. Thus, hearing your perspectives on those themes today is important. The second thing I would like to talk about is an area in which I have been doing research. These are the emerging trends in new account fraud detection for applicants on the Internet, where businesses are not physically present to authenticate the identity of customers. As everybody here knows, this is an area of growing interest throughout the banking industry.

Findings from the roundtable discussion on retail payments fraud

Let me start with the roundtable that the Federal Reserve sponsored last year. Fourteen industry experts—including merchants and representatives from payments system providers, financial institutions, and law enforcement organizations—participated. Overall, these leaders agreed that, although the current level of payments fraud is being effectively managed and does not represent a crisis, organizations must constantly adapt to keep pace with criminal activity and with changes in technology and payment methods. While the dollar amount of fraud relative to business revenues in the United States is likely declining, the costs associated with fraud mitigation are substantial and increasing. The roundtable discussions focused on four main themes: 1) the changing landscape of retail payments fraud, 2) current trends, 3) emerging concerns, and 4) areas for improvement in fraud detection and prevention. The following paragraphs sum up our discussions involving these four themes.

The changing landscape of retail payments fraud

Despite declining use of checks across the country, industry leaders find that the largest number of fraud attempts remains in check payments. Fraud losses are also highest for checks on a comparative basis with other payment methods. A number of participants stated that business losses resulting from check fraud are significantly higher than losses from noncheck payment types because checks are relatively easy to alter or forge, using readily available printers, scanners, and computer software.

Moreover, changes in the payments system and in criminal behavior have introduced additional risk. One key change in the payments system has been the proliferation of commerce conducted over the Internet. The Internet has created new means for criminals to gain access to consumers' personal and financial information, and has facilitated the formation of extensive illegal networks through which criminals buy and sell this information without the limits of geography. Indeed, substantial Internet fraud operations are now linked to sites located in certain developing countries. The Internet has also accelerated worldwide information-sharing among criminals regarding successful fraudulent schemes, so that new fraud techniques now move quickly around the world. In addition, the growth in online commerce has led to an increase in the number of transactions in which merchants are not physically present to authenticate the identities of purchasers.

Steve Malphrus is the staff director for management at the Board of Governors of the Federal Reserve System.

That said, some changes in the payments system have helped reduce risk, such as faster clearing of check payments associated with Check 21[1] and check-to-automated-clearinghouse (ACH) conversion. Being able to clear payments more quickly can mean that a fraudulent check may be returned before a collecting bank makes funds available to the depositor. At a minimum, faster returns help inform banks and their customers that fraud is taking place. But some feel that ACH e-check payments may be more vulnerable to fraud than other ACH standard code categories, such as ACH transactions initiated via telephone. Concerns were also raised over the greater use of check images in the rapidly growing Check 21 environment, which could reduce the usefulness of some current check security features that may not survive the imaging process.

Further, criminals' ability to adapt to changes in the industry's practices in fraud detection and fraud prevention is a continuing challenge, as these lawbreakers continue to seek the path of least resistance. For example, as large merchants and banks develop new tools to detect and prevent fraud, criminals turn to small- and medium-sized enterprises because they are less likely to have the resources to invest in fraud detection and prevention. Because fraud affects the entire financial industry, some feel that it is the duty of larger businesses and banks to reach out to educate and aid smaller organizations. Others suggest that we should raise the bar by increasing criminal penalties for fraud and prosecuting fraud more rigorously.

Current trends

It is becoming increasingly important for firms to protect consumer information. Industry leaders are concerned about the potential damage to their brands' reputations in the event of a data breach. The industry has taken steps to protect consumers from fraud that may result from compromised information. Often, for evidence of fraud, banks and card networks monitor customer accounts that may have been compromised and then reissue cards when necessary. Some industry leaders argued that, although the storage of data is a potentially vulnerable point in the payments system, the extent to which compromised information has actually been used is relatively low.

In many instances, if consumer information is compromised and subsequently used to commit payments fraud, the consumer is not liable for the associated losses. Thus, while it is important to protect consumer data, it is equally important to develop tools to prevent the fraudulent use of data or to otherwise render data unusable. One example is phishing.[2] While phishing is a current threat to the security of consumer information, many believe that the level of actual loss incurred from phishing has been relatively low in the aggregate. In some cases, education has been reasonably effective in preventing consumers from divulging information online.

In addition, it is important to differentiate between "payments fraud" and "identity theft." While both are a crime, the ramifications of each are substantially different. The Federal Trade Commission (FTC) has defined the term "identity theft" as fraud perpetrated by 1) obtaining access to and illegally using a consumer's existing financial information, such as a person's credit card number or bank account number, or 2) illicitly obtaining identity information about a consumer to open new financial accounts in the consumer's name. The roundtable participants generally agreed that the second part of the FTC's definition should be considered "identity theft" and that the first part should be considered "payments fraud." Some stated that the FTC report used an overly broad definition of identity theft, which has led to an overestimate of the true frequency of this type of fraud. Nevertheless, the consequences of true identity theft can be very significant for consumers. While actual financial losses might be low, the impact on a consumer's credit record—and the time and effort required to correct that record—can be substantial.

Emerging concerns

As noted, criminals are continually searching for weaknesses in fraud detection and fraud prevention practices. Several participants said that the potential movement of check-based fraud to the ACH network is an area of growing concern for the industry. A fraudulent payment initiated with a check can move into the ACH system through a point-of-purchase (POP), back-office-conversion (BOC), or accounts-receivable-conversion (ARC) transaction. Since ACH has traditionally been used for recurring payments from trusted sources only, banks may not yet have robust tools in place to detect fraudulent ACH payments from other sources. Fraudulent checks that may be detected using existing tools might, therefore, go undetected if processed on the ACH network. This possibility is a particular concern to businesses that use check fraud prevention services, such as positive pay,[3] that are not available for ACH payments. While a concern, fraud of this nature is, at present, relatively low.

The industry has only recently begun monitoring the movement of fraud across payment channels. Perhaps further study is required to understand how fraud is moving between paper and electronic instrument

or between different electronic instruments. Banks and businesses are looking to adopt a holistic approach to detecting and preventing retail payments fraud across the spectrum of payments systems. One participant described this approach as managing fraud at the "relationship" level—that is, at the level of an individual or a corporate client for a bank, and a customer for a merchant—rather than at the "product," or payment instrument, level.

Moreover, the industry is concerned that the introduction of new payments instruments, such as prepaid cards, could increase fraud in the payments system. One participant noted that some of these cards can be easily reloaded with funds and can be used anonymously, making them effective vehicles for money laundering. Another stated that open-loop, reloadable prepaid cards could be a primary vehicle for fraud in the future, and others concurred that prepaid cards are a growing area of concern. We also discussed the security of mobile and contactless card transactions. On the one hand, payments made using these devices could be more exposed depending on their security features. On the other hand, the development of security enhancements, such as "dynamic" authorization techniques, for some payment devices can offer significant benefits. The hesitation in trusting emerging payments instruments may stem from the fact that their risks are not yet understood. Successful payments systems have historically had to put innovative systems into production and undergo a learning phase before the development of a fully mature risk-mitigation strategy.

Areas for improvement in fraud detection and prevention

At the roundtable, the most discussed suggestions for improving the industry's ability to detect and prevent retail payments fraud were 1) increasing industry collaboration and information sharing, 2) using enhanced authentication techniques, and 3) adopting Payment Card Industry (PCI) standards.

Merchants and financial institutions could benefit from increased collaboration and information sharing across industries and within their own business sectors, including through the development of best practices in fraud detection. Firms need to not only detect fraudulent transactions in process but also prevent fraud's initial occurrence by improving authentication at the point of sale. At the roundtable, the effectiveness of PIN (personal identification number) and chip technology was debated. Some stated that fraud rates on PIN debit cards are significantly lower than those for other payment types; as a result, they advocated the application of PIN security to card payments in general. Chip technology has been widely adopted in other countries, and could prove to be a safer alternative to magnetic stripe technology for card-based transactions.

Roundtable participants also discussed the role of the Payment Card Industry program, developed jointly by Visa and MasterCard. Full compliance with security standards could help the industry safeguard consumers' personal and financial information. The PCI program in particular could be helpful, but there are challenges for some organizations to become compliant with the PCI program. Nevertheless, compliance with the PCI program might be a good first step in securing consumer information, though other opportunities exist. For example, existing data privacy regimes generally apply to banks or merchants, while they exclude others, such as third-party service providers. These third parties have access to consumers' personal and financial information. In order to improve the security of consumer information, it is desirable to expand data protection regimes with respect to both the types of payments and the types of organizations that are included.

Ultimately, the roundtable discussions returned to the refrain that criminals will continue to search for the fastest and easiest ways to commit payments fraud. Consequently, strategies for fraud detection and fraud prevention should be considered holistically, so as not to merely shift fraud from one payments channel to another. Industry leaders maintain that it is not financially feasible to prevent all payments fraud. Rather, businesses must make prudent, risk-based decisions that will yield appropriate returns relative to the investment required to minimize fraud. Organizations continue to balance costs and benefits when investing in tools to mitigate fraud.

At the roundtable's conclusion, several suggestions emerged for how the Federal Reserve might assist the industry's efforts to mitigate fraud. Some advised the Federal Reserve to continue its outreach events to encourage industry participants to share concerns and effective practices, and others emphasized the importance of the Federal Reserve conducting research on payments and fraud-related issues. As a general matter, however, leaders advocated the continued application of market-driven approaches to keep payments fraud at a manageable level. Payments system participants' ability to adapt to changes in criminal behavior will be critical in maintaining a safe and efficient payments system.

Some thoughts on new account fraud

Shifting gears now, I would like to offer my perspective on recent developments in the detection of

fraud in new accounts. Many companies with an online presence today are struggling to find solutions for screening out fraudulent applicants for new accounts. These accounts range from those used for banking and brokerage accounts to accounts used for services. The dilemma is universal for online businesses where there is no person-to-person discussion with the applicant and, therefore, no possibility to examine documents such as driver's licenses or passports and to verify identity in person. New account fraud in such non-person-to-person (mainly online) environments is estimated by some experts to be four to five times higher than it is when accounts are opened in person.

Although there is no comprehensive solution available in the market today, various methods can help detect accounts opened for illicit purposes. In the case of regulated banks, meaningful attempts must be made to detect new account fraud under the new "red flags regulations" that were fully implemented by November 2008 (I discuss these regulations in greater detail later). This is true whether the ultimate victim is a consumer, whose identity has been stolen, or the business itself, where an account is opened using a fictitious identity created by a criminal.

Client device identification

In the non-person-to-person online environment, a business does not have an opportunity to screen identity documents, videotape the person, and/or engage directly with the applicant. However, the business does have an opportunity to screen the user's device, such as a personal computer. Various technologies make device identification and analysis a useful first step in flagging suspect applicants. For first-time users, businesses can obviously not rely on installed desktop software, tokens, or credentials that have already been installed. However, they can analyze various pieces of information available through the user's web browser connection to check for potentially fraudulent activity. These include the following.

- *Geolocation* of the user based on the user's Internet protocol (IP) address. Vendors that specialize in IP address intelligence are often able to detect the use of blacklisted IP addresses or blocks of addresses (that is, those that have been known to be used for criminal activity). They can detect the use of anonymizers and/or proxy servers that criminals use to hide their locations. Businesses can also compare the country and geographical region of the IP address to the country and region from the user's credit card billing address.
- *Personal computer/web browser identification* examines the hypertext transfer protocol (HTTP) browser header and other information from the user's computer or device, and compares them to what are expected. For example, this process can compare the time stamp from the computer to the time expected from the user's geolocation. Using a JavaScript executed from the business's server, this software can try to uniquely identify a computer and determine if it is being used by a large number of account applications. Software is available today that specializes in computer identification using proprietary techniques along with geolocation analysis. Similarly, a biometric system that records a user's keystrokes and unique typing pattern can be used to ascertain if the same person, and not just the same machine, is opening multiple accounts.
- *Botnet detection* can identify a machine on a criminally run botnet that is accessing an enterprise's website.

Fraud detection using information on the account application

Device identification tests can be subject to further fraud screening through the use of information entered on the application. Depending on the information requested on the application form, these fraud detection strategies can include the following.

- *Identity proofing,* which is typically used when a comprehensive set of information is being requested from the user, such as financial data, Social Security number, employment history, and home-ownership information. This is common when applications are filled out for financial accounts, such as insurance, credit card, and bank accounts. Identity proofing can be relatively expensive, at a few dollars for each identity checked, and uses either:
  - Rule-based data-matching systems from vendors or credit bureaus; or
  - Identity scoring, relying on service and software providers that detect potential fraud using scoring models that look across application records and data.
- *Credit card fraud detection,* which is useful for new account openings that require only a credit card authorization. This detection typically costs about 15 cents to 25 cents per transaction, on top of the usual authorization costs, and depends upon

volume and vendor-licensing arrangements. These systems analyze data available from credit card records, such as billing address and shipping address. They perform various checks, such as validating addresses using the card companies' address verification system, and compare credit card billing and shipping addresses to the customer's geolocation and to lists of suspect addresses. The systems check to see how many times the end-user accesses a webpage asking for credit card information—possibly an indication of a brute force attack against a card's security code. Credit card fraud detection systems also can compare credit card numbers provided by the user with stolen cards noted on blacklists, although stolen credit cards are so readily available to the fraudsters that blacklists have limited value. Most systems for credit card fraud detection enable enterprises to manage the business rules that each of their transactions runs against, so the businesses can catch fraud patterns particular to their situations.

- *Niche data verification*, which refers to the verification of specific data, such as telephone numbers or applicants' ages. These data are then reconciled with data expected from the applicant. The line information database is a telecommunications industry standard database containing the same information made available through hub providers. Unfortunately, it is still not possible for enterprises to get access to a comprehensive set of wireless phone directories held privately by some wireless carriers (notably Verizon Wireless)—a step critical in verifying phone numbers because many customers prefer listing cellphone numbers rather than landline numbers.

Stepped-up applicant verification

Optimally, all account applications should go through a set of initial screening procedures, and suspect transactions that need further review should be routed to a fraud investigation queue for manual or automated follow-up. Additional automated screening can occur using one of the following methods.

- *Identity proofing* is a method that uses knowledge-based authentication systems, based on public source data that pose questions to the user that only he or she can presumably answer (such as "What was the make of the first car you owned?"). Vendors offer identity-proofing applications based on public records, which can be partially effective in screening out fraud. However, roughly 20 percent of the question/answer sessions invoked for high-risk applications fail or are abandoned. Sometimes, the failure is because legitimate users cannot successfully answer the questions or because there is not enough public data available for a particular individual. At other times, criminals manage to answer questions successfully.
- *Telephone-based user verification* is a method that relies on a call to an applicant using a phone number found in the public records or provided by the user personally. The automated phone system can simply ask the user to speak, and it can record the user's voice or ask the user to type in the phone transaction number generated by the online application session. This method is not foolproof unless the business is sure that the phone number on record belongs to a legitimate user.

Implications of red flags regulations

On October 1, 2007, the Federal Trade Commission and federal banking regulators, including the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration, released rules that require financial institutions to step up efforts to combat identity-theft-related fraud. These long-awaited identity theft rules implement the Fair and Accurate Credit Transactions Act, or FACT Act, and took effect on January 1, 2008. Financial institutions covered by the rules had until November 2008 to comply.

The rules require regulated financial institutions to create "reasonable policies and procedures" for detecting and preventing identity theft. Red flags cited in connection with an account application or an existing account include patterns of activity that are inconsistent with the historical and usual pattern of an account, such as a recent and significant increase in inquiry volume or an unusual number of recently established credit relationships. Other red flags include applicant addresses that do not match addresses from external sources, as well as internally inconsistent personal information, such as a lack of correlation between the Social Security number range and the date of birth. Institutions are also asked to check for invalid phone numbers or addresses and to flag applications for which an address, Social Security number, or phone number provided is the same as that submitted by other persons opening an account or by other customers.

Conclusion

As we ponder retail payments fraud going forward, the risk is not just about the cost of dealing with fraud and the associated losses. Indeed, fraud risks and associated retail payments fraud will cross into areas of public policy related to privacy. Today privacy is becoming a serious issue, and interestingly, this issue brings us full circle to the broader topic of information security.

Government agencies, for example, have a new mandate in terms of handling information about citizens: It is called private identity information. Federal agencies must take affirmative action to protect private information such as Social Security numbers, dates of birth, etc. Moreover, today the U.S. Department of Homeland Security has an assistant secretary for cyber security and communications. That position centralizes the federal government's work in this area as well. Other agencies that work on privacy and identity issues related to payments fraud include the Central Intelligence Agency, the National Security Agency, U.S. Department of the Treasury, and the Federal Reserve System. Concerns about terrorist financing and money laundering drive much of this federal work, but we should remember that such concerns are also increasingly spilling over into the world of payments fraud. In the future, you should see additional coordination and partnerships between the public sector and the private sector to address risk.

I think it is important to understand that the Federal Reserve System is unique in that it acts as a banker's bank, the federal government's bank, and a payments system operator. Having a payments system that is safe and secure is an absolute necessity in maintaining the confidence and trust held in it. To achieve this, we must focus on operations risk first, but also pay attention to reputational risk. It is important for us to understand these risks from multiple perspectives—from the economic research perspective, from the perspective of a financial market authority, and from the perspective of a very large bank.

NOTES

[1]For details on the Check Clearing for the 21st Century Act, see www.federalreserve.gov/paymentsystems/truncation/.

[2]A phishing attack uses randomly distributed emails to attempt to trick recipients into disclosing personal information, such as account numbers, passwords, or Social Security numbers. See www.spamlaws.com/online-credit-card-fraud.html.

[3]Positive pay is an antifraud service offered by virtually every U.S. commercial bank. It protects a company from altered checks and counterfeit check fraud by comparing the components (such as the account number, check number, and dollar amount) of each check presented for payment against those from a list of checks previously authorized and issued by the company. It allows a company to reject unauthorized transactions (that is, for checks that do not match) before losses occur.