Current Fraud Management Techniques in Consumer Lending

by Michael E. Collins

The answer: Stringent measures and strong data protection by merchants, card issuers, and cardholders, as well as an environment of risk awareness in the industry. The question: What can substantially mitigate the threat of fraud in consumer lending? The consequences of a different answer: Jeopardy! In this article, the author provides an overview of mitigants for consumer fraud based on trends observed by the Federal Reserve Bank of Philadelphia.

Consumer lending has been a growth engine for the commercial banking industry for the past few years. In the last three years alone, consumer loan outstandings have grown 45% and now represent almost 54% of total loans. Along with all of the usual risks in lending, such as underwriting, debt service/repayment, and interest rate risk, consumer lending—especially credit card lending—presents additional challenges with regard to fraud. Moreover, statistics show that fraud in consumer lending continues to increase. For example, a survey report by the Federal Trade Commission (FTC) estimated that identity theft losses over a 12-month period in 2002 and 2003 totaled $47.6 billion for businesses and $5 billion for consumers.

As a banking regulator in the Third Federal Reserve District, the Philadelphia Fed closely watches fraud trends in the consumer lending industry, since 36% of all managed credit card receivables emanate from Delaware-based institutions. Poor control by an issuing bank over PINs, return mail, credit limit increases, and name and address changes can contribute to credit card fraud.

What can be done to stem the increase in fraudulent credit card activity? For a start, three key players must take stringent measures to prevent fraud: merchants, card issuers, and cardholders. In addition, strong data protection practices at each level and an environment of risk awareness in the financial services industry can also substantially mitigate the threat of fraud.

Merchants/Point-of-Sale

Preventing credit card fraud at the point-of-sale may not be as easy as it sounds. Although many people still buy goods and services in the brick-and-mortar retail world, more and more people are buying items in the virtual world of the Internet. Transactions over the Internet are harder to authenticate and therefore make fraud...
prevention trickier. However, many companies have established techniques to lower the risk of credit card fraud over the Internet.

In person. For in-person retail transactions, merchants can do at least three things to prevent credit card fraud. They can ensure that the customer initiating the transaction is authorized to use the credit card by verifying the card user’s signature. Unfortunately, many merchants are reluctant to be too aggressive in trying to verify a customer’s identity because they fear damage to their reputation will result if a customer is falsely accused of credit card fraud.

It also is incumbent on merchants to implement and enforce measures that control access to card readers and customer information. Furthermore, merchants must have confidence in the honesty and integrity of their employees.

Internet. The virtual world presents many opportunities for credit card fraud. Consequently, companies have developed a number of fraud-prevention techniques to deal with the additional risks of online transactions. One such technique is the use of card verification value\(^3\), which requires the customer to provide the three digits found on the reverse side of the credit card before initiating a transaction. (American Express cards use a four-digit number found on the front of the card.) Because these digits are not embossed and, therefore, do not appear on a receipt, having the customer provide these digits adds another layer of assurance that the person initiating the transaction is in possession of the card.\(^4\)

Another technique for protecting credit card transactions over the Internet involves account number masking, also known as substitute credit card numbers or virtual account numbers. Such a technique helps prevent criminals from intercepting and stealing the real credit card number. To use this technique, the customer has to go to the card issuer’s Web site to start the transaction. In turn, a new card number is established and sent to the merchant’s site for the purchase, thus keeping the original credit card number secret.

Since merchants cannot verify a customer’s signature in the virtual world, typically the merchant is responsible for fraud chargebacks.

Biometrics. In the future, merchants may be able to use even more sophisticated methods to prevent credit card fraud. Although many of these technologies are currently available, each has had varying degrees of acceptance, and some require substantial up-front investments. Whether used independently or to supplement existing security measures, such as those embedded in smart cards, biometric technologies offer merchants at the point-of-sale legitimate alternatives for protecting themselves and their customers against illicit criminal activity, such as identity theft, account manipulation, and fraud.\(^5\)

Following are some of the more widely used biometric solutions.

• **Fingerprinting.** Because of its reliability and cost effectiveness, fingerprint scanning is the most widely used biometric application today, accounting for about 50% of the overall market.

• **Voice recognition.** Voice recognition technology remains a second-tier alternative among current biometric alternatives. Despite difficulties with the voice compression associated with microphones and handsets, voice recognition is useful for remote authorization through phone lines.

• **Iris/retina scanning.** This technique is an attractive alternative because of its accuracy, but start-up costs are extremely high.

• **Facial recognition.** This technique analyzes the characteristics of an individual subject’s face image, including facial structure and spatial measurements between the nose, eyes, jaw, and mouth.

Card Issuers

Since card issuers bear the brunt of the costs of fraud in face-to-face transactions, they have the most interest in preventing it. Like the merchant, the issuer has to be concerned with verifying the customer’s information. In addition, the issuer has to be sure that the customer’s information remains secure when it is stored. The issuer’s first opportunity to detect and prevent fraud comes during the application process.\(^6\)

The simple practice of confirming an applicant’s information through multiple data sources is a good start. Many issuers may also perform phone/address distance calculations to determine if the area code on the application matches the address. Some computer pro-
grams can segregate high-risk applications for a detailed review, using the applicant’s geographic location or other special characteristics.

The card-activation process typically has fraud-prevention controls built in. When a cardholder calls to activate a card, a flag may be raised if the call does not originate from the home phone number on the application. As an added screen, those calls can be rerouted to a customer service representative, who can attempt to verify the caller’s identity.

Other fraud-prevention techniques use sophisticated neural-network software to determine unusual transactions. Such activity ranges from sudden and extraordinary usage of cash advances after a new account is opened to large-dollar purchases at a location far removed from the card holder’s normal purchasing area. These techniques continue to advance as more data and history are gathered.

Cardholders

Many card issuers realize that their first line of defense lies in the hands of their customers. As a result, card issuers and many other organizations have produced and distributed literature to aid customers in protecting themselves against fraud.

We need only watch television to see how important fraud prevention is to the credit card industry. Some of the most talked-about commercials are produced by credit card associations and issuers to address identity theft. Institutions have started to market products based on their ability to protect the customer from fraudulent transactions, rather than just on price and convenience. Some companies have even created new products, such as the Blue Card from American Express and Verified by VISA, to address customers’ concerns about fraud.

The FTC, realizing the importance of consumer awareness, has published a number of fraud-prevention documents specific to credit card payment fraud. “FACT S for Consumers: Avoiding Credit and Charge Card Fraud” provides a list of best practices for consumers:

- Sign your cards as soon as they arrive.
- Carry your cards separately from your wallet, in a zipped compartment, a business card holder, or another small pouch.
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your card during the transaction, and get it back as quickly as possible.
- Void incorrect receipts.
- Destroy carbon receipts.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Report any questionable charges promptly and in writing to the card issuer.
- Notify card companies in advance of a change in address.

Fraud and Enterprise-wide Risk Management

An enterprise-wide risk management program helps organizations manage risk, making risk assessment an integral part of an organization’s strategic and tactical planning. It is clear that fraud prevention is an essential component of consumer lending and, as such, remains a major focus for credit card companies because of the high cost of fraud to their core business strategy. Fraud prevention and compensating controls have always been important components in managing operational and credit risk and should be integrated throughout an organization’s enterprise-wide risk management activities.

Organizations should be proactive in reducing opportunities for fraud by identifying and measuring fraud risk areas, taking steps to mitigate identified risks, and implementing and monitoring appropriate internal controls and other deterrent measures. Credit card issuers in particular must be particularly vigilant and must institute proper controls throughout all card-issuing and transaction-processing activities. Reviewing possible causes of recurring malfunctions in pay-
ment authorization systems should be a standard practice, along with on-site inspections of merchant operations and reviews of contracts with third-party providers and marketing agencies.

Despite all of the efforts to prevent and detect fraud, combating credit card fraud remains a challenge. Banking organizations must work continuously to stay ahead of large global crime syndicates, and many of the detection and security practices common in the U.S. are not as robust outside our borders. As markets for consumer credit expand globally, fraud prevention and risk management practices must be rigorously applied to prevent potentially significant losses.

Management’s Role

In 2002, the Auditing Standards Board issued Statement on Auditing Standards 99 (SAS 99), Consideration of Fraud in a Financial Statement Audit, to identify practices that could help an external auditor detect fraud during a financial statement audit and to more clearly define the role of the external auditor in detecting fraudulent activities. While such a review during an audit is important, management and the board of directors are in the best position to deter and/or prevent fraud before it even occurs. An exhibit to SAS 99 discusses anti-fraud programs and controls that an organization’s management could implement in the context of the following three fundamental elements:

1. Creating and maintaining a culture of honesty and high ethics.
2. Evaluating the risks of fraud and implementing the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud.
3. Developing an appropriate oversight process.8

Management is responsible for designing and implementing systems and procedures for preventing and detecting fraud and, along with the board of directors, for creating an environment that promotes honesty and ethical behavior. This includes ensuring that staff at all levels are educated about the fundamentals of controls and their importance in deterring fraud. But, ultimately, fraud prevention and detection remains the responsibility of the audit committee and the board of directors.

Only those organizations that seriously consider fraud risks and take steps to create a climate to reduce the occurrence of fraud will be successful in preventing fraud.

Michael Collins may be contacted by e-mail at Mike.Collins@phil.frb.org.

Notes

1 Consumer loans include first and second mortgages as well as home equity lines of credit, credit card receivables, securitized credit card receivables, and installment loans.
4 This fraud prevention technique is also used in telephone transactions.