Back to Basics

By Roy W. Urrico

Take Charge

Gaining Control of Chargebacks

Minimizing or eliminating fraudulent chargebacks is an investment in current and future business. Merchants protect their bottom line and customer base, and independent sales organizations (ISO), acquirers and processors protect against credibility loss.

Participating financial institutions, card associations, merchants and the merchant's bank all agree to the credit card system rules regarding chargebacks. Under this scheme, a financial institution can overturn a transaction within a specific period.

There are two types of chargebacks: procedural and substantive. Procedural disputes are raised by issuers for reasons relating to the form of the transaction or some error in processing. For this column, we'll focus on substantive chargebacks. Examples of substantive chargebacks are: unauthorized transactions, undelivered goods or services, or dissatisfaction with delivered goods or services.

Credit card associations offer cardholders the power to challenge charges that occur due to theft, fraud or error. Fraudulent charges that result in transaction reversals can transpire with or without a cardholder's knowledge.

"A merchant will lose revenue from two types of chargebacks," says Ted Svoronos, vice president of e-commerce for StrikeForce Technologies, which provides authentication solutions — chargebacks related to identity theft and opportunistic charge reverses from individuals not wishing to pay for goods.

Either way, it is bad news for merchants. Merchants not only lose the product and the sale but also must pay a chargeback fee (sometimes $10 to $30) to the issuing bank.

Point-of-sale (POS) chargeback rates are approximately 1 percent of all sales. Possible chargebacks for online sales are greater, so the hazards for banks and merchants increase as well. That explains why for every fraudulent transaction that occurs online, two to three are turned away because they look fraudulent, explains Svoronos.

The bad news does not stop there. A chargeback resulting from identity theft will probably wind up with the consumer whose identity was stolen losing confidence in the merchant.

For ISOs, acquirers and processors, a run of chargebacks could affect their standing in the transaction supply chain, according to Svoronos.

"Everything is based on credibility and credit history," he says.

Card associations identify acquirers that cannot control the ratio of fraud volume or chargebacks. Acquirers also can be subject to hefty fines and lose their Merchant Credit Accounts.

Speed Up the Process

Last summer, Visa announced that it had begun implementing system upgrades. The upgraded systems are expected to expedite the process for resolving cardholder purchase disputes through improved automation and communication, streamlining rules and procedures, and using electronic transmission in place of paper documents and the mailbox.

The Visa initiative was named Re-Engineering Disputes (RED). Visa Resolve Online, a Web-based tool, is considered a key component of the initiative and is expected to play a major role in speeding the dispute resolution process. Most cardholder disputes will be resolved within just one billing cycle.

"All stakeholders will benefit from a dispute resolution process that provides them with better access to information, more options for communicating and ultimately faster resolution of their

Common Reasons for Chargebacks

Visa International offered some of the more common reasons chargebacks occur at the point of sale (POS):

- ***Non-receipt of requested copy.*** This is when a financial institution requests a copy of a transaction receipt from a merchant about a disputed sales charge. If a customer has been charged incorrectly or the merchant fails to respond to the copy request by the due date specified, the merchant is subject to a chargeback.
- ***Duplicate transaction.*** This is usually the result of a customer claiming to be double billed for the same transaction.
- ***Missing signature.*** In a face-to-face transaction, not obtaining a customer's signature could result in a chargeback claim.
- ***Missing imprint.*** A transaction can be reversed without a clear, legible imprint.
- ***Expired card.*** Accepting a card that has expired may result in the sale being charged back.
- ***Canceled recurring transaction.*** Processing an automatic transaction after a customer has canceled the arrangement.
- ***Authorization was declined.*** Merchants may be charged back for a transaction when authorization was requested but declined and the transaction was processed anyway.

disputes," said Dave Van Horn, vice president of Visa USA in a company statement. This transformation represents a mutually beneficial solution to dispute resolution issues, he added.

According to Van Horn, initial system upgrades were a significant factor in the 21 percent decline of chargebacks in 2002, resulting in approximately $238 million less in losses, a significant savings for merchants.

Identify Theft

The most common reason for chargebacks when it comes to mail, phone and Internet orders is non-possession of a card. This is because, in most cases, transaction approval is based on having a credit card number and an expiration date.

"We are authenticating a credit card. ... [We] are never identifying the user of the card," says Svoronos. "You can minimize and possibly eliminate [chargebacks] by not automatically approving a card online. ... Receiving just a credit card number and an expiration date does not validate an identity," he adds.

This is particularly problematic for the e-commerce chain, with ID theft costs at an all-time high.

According to the Federal Trade Commission:

On average, victims of "new accounts and other frauds" ID theft indicated that the person or persons who misused the victim's personal information had obtained money, or goods and services, valued at $10,200 using the victim's information. This result suggests that the total loss to businesses, including financial institutions, from this type of ID theft was $33 billion in the last year (2002-2003).

Adding the costs that resulted from "misuse of existing credit cards and credit card accounts only" ID theft and from "misuse of other existing accounts" ID theft to those from "new accounts and other frauds," the total cost of this crime approaches $50 billion per year, with the average loss from the misuse of a victim's personal information being $4,800.

Chargebacks also result from confidentiality violations. "Privacy infringements are not necessarily a result of chargebacks but rather chargebacks are a result of privacy infringements," says Howard Cohen, president and CEO of My Virtual Card, a StrikeForce Technologies partner.

Stop Fraudulent Chargebacks

StrikeForce Technologies has developed a solution called Centralized Out-of-Band Authentication Solution (COBAS), designed to stop chargebacks by verifying identities in brick-and-mortar transactions or online purchases. "The problems with ID theft and fraud is you are not catching it at the outset," says Svoronos. "We are a proactive system."

StrikeForce believes there is a fundamental fatal flaw in existing computer security — the pairing of usernames with credentials (identifier) sent over vulnerable network pathways. Regardless of the password scheme or device, tying a username with authentication acceptance makes hacking possible.

In a typical connection, the user sends a message asking a secure server to grant access. The server then replies with a request for the client to supply its credentials (identifier or identity). Once that information is received, an authentication process takes place. The server returns the authentication approval or denial to the user using the same vulnerable network path.

From that moment on, says Svoronos, the username and credential (identifier) are inextricably linked. Once a hacker has a user's identifier, a piece of the security equation, it is only a matter of time to get the other. The COBAS model creates a separate "out-of-band" pathway for authenticating a user's credentials, away from the client network and out of reach for hackers or intruders.

"Our technology authenticates each and every transaction... We eliminate the identifier and obtain the identity...you have to verify the identity, " adds Svoronos.

COBAS has an open architecture platform that serves as a central point of control and management of domain, virtual private network (VPN) and Web access — with an ability to layer biometric devices. "Our solution is simple and sophisticated," says Svoronos. "This offers credit card companies and cash card companies the ability to use our technology to stop ID theft."

Among Strike Force's partners is Centipaid, which uses COBAS to integrate parental control and spending limits to its digital cards using StrikeForce out-of-band technology. "Our software sits inside any organizational network," explains Svoronos. "When a transaction comes up our software goes to work instantly." COBAS can be set up onsite or be outsourced. For example, Panasonic built a facility just to handle transaction authentication.

Ramifications

If chargebacks and fraud are not better managed, there are enduring and mounting threats to merchants' bottom line, which carries over to ISOs, acquirers and processors. This is particularly true for e-commerce. "Only 5 percent of people with computers do online transactions," says Svoronos. "They are scared to death."

From a business perspective, the online fraud issue may be overblown, according to one industry source. Financial Insights, a research and advisory firm, reported last July that merchant participation in Verified by Visa — a program that protects merchants from fraud liability — is lagging. The main reason: contrary to popular opinion, online fraud is not yet a major U.S. problem. "While protection from chargebacks is important, the largest merchants already have low fraud rates and will need lower interchange rates to see value from the technology," says Aaron McPherson, research manager of retail payments at Financial Insights. **TT**

Roy W. Urrico is editor of the Association for Financial Technology newsletter.