

# A Compromising Position

Practical advice for protecting customers after bankcard data breaches



By Alan Nevels

A breach of credit or debit card data that compromises customers' card information—like the recent TJX Cos. Inc. incident where fraudsters stole thousands of card numbers and related information—often prompts community banks to instinctively reissue all potentially affected cards.

But an auto-card reissue policy may not always be justified, especially when actual fraud loss as a result of security breaches is low. In deciding whether to reissue, community banks need to consider all of their options as well as the possible ramifications for their customers.

While the bank's financial interests and customers' security is always a foremost priority, since financial liability almost always resides with the bank to cover any customer losses, community banks must also be mindful of the possible inconvenience and the

overall impact that reissuing cards will have on customers.

Customers whose credit access has been suspended (sometimes for as long as 10 business days in cases involving large data breach events) not only have to wait for new cards, but also have to endure the inconvenience of calling service providers or retailers with whom they have automatic payment arrangements to switch the card account number. Many community banks with automatic reissue policies find that they are issuing cards to the same customers sometimes two to three times per year, and as a result their customers either use a competitor's card to transact or customers move their banking relationship all together.

Reissuing cards also comes at a price for the bank. Depending on the service agreements in place, banks can plan to spend \$5 or \$6



for each new card plastic alone. Visa estimates the total cost associated with reissuing a card (including plastics cost, mailing cost, employee time and monitoring cost) can exceed \$20 per card in some cases. Multiply that by 2,000 or 3,000 customers and the cost becomes significant.

A figure harder to quantify is the lost revenue for the time a bank's card is out of play. It's more likely customers will switch to another card, at least during the period when a card is blocked, than suspend their card usage. So banks also lose interchange revenue when they choose to block accounts.

In some cases, the bank must encourage its customers to return to using its card when the new card is received; a harder task if the bank constantly reissues cards and is blamed for any inconveniences even if an outside party, such as a retail chain, causes the problem. "Since every security compromise is unique and no two institutions are alike, banks must weigh each exposure separately to determine the best course of action," says Michael Smith, senior vice president of Visa USA.

Smith said new technologies can help a bank assess the risk of not issuing each card by detecting transaction patterns that would indicate whether fraud has occurred or is likely to occur with a given card. These technologies enable banks to focus only on cards that pose the greatest risk.

The first thing banks should do is to keep an eye out for the account compromise alerts issued by Visa and MasterCard. These alerts not only provide the numbers of cards that may have

## Getting the Word Out



Informing your customers about how they can lower their risk of fraudulent activity can lower your bank's costs, too. Cardholders who routinely check their account balances online are likely to spot questionable charges. Encourage your bank's cardholders to review online statements for suspicious activity. Tell your customers about their card's transaction-liability policies.

Also, make sure that your bank's staff is well aware of major security breaches and that they can explain to customer what the bank is doing to protect their security.

been compromised during a detected security violation, but they provide other valuable information about what data was obtained via the compromised files. Such data can greatly assist banks in assessing how serious the risk is to each card.

"If a criminal just got customer names, card numbers and expiration dates, that is less risky than if they got the entire mag-stripe data. With the latter, criminals can duplicate cards and use them," says Paul Weston, president and CEO of TCM Bank, N.A., a limited-purpose credit card bank of ICBA Bancard Inc.

In addition to looking at what information was stolen, banks need to look closely at the expiration dates of the cards and the date on which the security compromise occurred. "During a recent security breach at TJ Maxx, criminals obtained data that went back to 2003. A lot of those cards may have already expired, and if so, they present little danger," Weston says.

If a bank chooses not to reissue all of its cards, there are tools that can be used to monitor the activity of designated cards with a greater scrutiny than other cards. That's where Visa's Advanced Authorization Service comes in.

The Advanced Authorization

Service provides a risk code for each transaction made through the Visa payments system, and cards that are suspected of being compromised are assessed a higher risk score. It scores the risk associated with each card, based on the transaction type and any historical information known in Visa's CAMS (Compromise Account Management Services) alerts.

"When we see a reported breach we can tweak the parameters for authorizing a transaction on cards that were affected," Smith says. This allows a bank to adopt a more conservative approach to approving transactions on cards potentially affected by compromised data.

Banks that issue their own cards will be required to use this tool beginning in April, and those using third-party processors can receive the tool through them.

In addition to Visa's Advanced Authorization, ICBA Bancard is piloting the use of a real-time model of its current Falcon fraud tool, our version of the neural network system that looks at the risk associated with each card transaction. What makes real-time Falcon different from what is currently modeled

for ICBA Bancard issuers is that Falcon now detects a pattern of fraudulent behavior and flags transactions that are believed to be fraud-related after several fraudulent transactions have been already approved. With the new version, Falcon will score risky or suspect transactions right at the point-of-sale during the first transaction.

“Previous fraud detection was designed for petty crooks who would steal cards from purses and wallets,” Weston says. “Today organized crime is breaking into computer systems and stealing thousands of card numbers. If you allow two or three bad transactions per card, the cost could be staggering. You have to stop the fraud during the first or second transaction.”

Another thing to consider prior to reissuing a customer’s card is to look at account activity. An account with a lot of activity will cause greater inconvenience to the cardholder if the bank blocks the account and reissues the card. And look at re-issuance timeframes. If a card is about to expire shortly, accelerating the re-issuance time by a few months may make sense. On the other hand, if a customer was just reissued a card, reissuing another one may not be the best policy if other risk factors are in line.

Education also plays a key role. Banks should talk to their customers about how to lower the risk of compromised-related cards. Engage your customers to help monitor their own credit and

debit cards via Web-based card solutions. With a strong commitment to assessing “real risk” and the use of advanced technology, banks can protect their customers and themselves from fraud without undergoing the unnecessary expense and

troubles associated with reissuing every card reported in a compromise event. **ib**

---

*Alan Nevels is senior vice president of operations and card risk for ICBA Bancard. Reach him at [alan.nevels@icba.org](mailto:alan.nevels@icba.org).*