

Comprehensive Fraud Protection

Credit card issuers seek heightened data security.

By Preston Faykus

With the rise in the use of plastic as a preferred method of payment comes a correlated rise in fraud risk. Card-issuing financial institutions, large and small, combat this nemesis continually. While larger issuers obviously have greater exposure due to the sheer volume of cards issued, community financial institutions have increasingly become the targets of fraud as well, having grown their card portfolios significantly to become bigger players in the card industry. Looking for new fraud opportunities, fraudsters are operating under the misguided notion that community financial institutions are somehow less protected than the megabanks. In fact, financial institutions of all sizes now have



dedicated fraud prevention teams and are pursuing the latest technologies in their ongoing battle against data theft.

Financial institutions, large and small, must allocate the necessary resources to combat and prevent fraud. In the unfortunate instance of a breach, these resources then must shift their focus to post-breach efforts, which include block and re-issue decisions, risk-exposure analysis, and cardholder communication options. These efforts can be extremely time-consuming, cumbersome to manage and costly, often requiring additional staffing resources and time commitment.

Fraud Goes High-Tech

As payment card transactions have increasingly become electronic, fraudsters have capitalized

on the vulnerability of unprotected electronic data and incorporated high technology into their own schemes. While the fraud of yesterday called “phishing” was fairly primitive and more of a nuisance than a threat, the “cloned” Web sites created by today’s high-tech fraudsters bear an incredible resemblance to the real Web site, making it very difficult for consumers to differentiate fact from fiction, and pose a significant challenge for those managing online payment security.

Whereas counterfeiting used to be a more localized event on a smaller scale, the high-tech capabilities of today’s criminal organizations enable fraudsters to identify and take advantage of weaknesses in retail inventory and accounting systems and circulate large numbers of counterfeit cards internationally—and within minutes.

The First Line of Defense

Like most problems, the best way to prevent fraud is to stop it before it starts. To do so, the first line of defense against card fraud is the authorization system. Critical fraud deterrence strategies, such as address verification service, CVV/CVC, CVV2/CVC2, and exact expiration date matching, should be active within the authorization system. When any data mismatches occur, the transaction authorization can be declined. Other less-common controls available include name matching, daily limits and using various parameters to block suspicious transactions, such as merchant category codes, country codes and dollar amounts.

By now, most institutions are aware of the enormous responsibility of maintaining data

integrity and understand the importance of having a comprehensive 24/7 fraud detection system in place. These neural networks should include rules-based processing, predictive fraud scoring and the ability to block authorizations in real time as they occur. Declining fraudulent transaction authorizations at the point of purchase is paramount because fraudsters typically stop using stolen cards as soon as their first transaction is declined.

Investigate, Challenge and Recover

In addition to pursuing every available avenue of recovery—including reviewing fraudulent transactions to ensure they were authorized if above the floor limit, requesting copies of the draft and obtaining affidavits of fraud from the cardholder—procedures should also be implemented to challenge incidents of “friendly” fraud and negligence, such as disclosure of a PIN.

In large-scale compromise events, Visa’s Account Data Compromise Recovery Process can help issuers offset compromise-related costs and potentially recover a portion of the losses associated with the re-issuance of cards. While this may help mitigate some of the expenses an issuer may incur as a result of a breach, it is not a panacea. Card associations must continue to pressure merchants to be responsible in the way they store data and to comply with industry standards.

Analytics on Confirmed Fraud

Spotting flash-fraud patterns and possible points of compromise requires that issuers be able to analyze broad ranges of data. This

data can consist of neural network scores, authorization level information, monetary and nonmonetary data, and fraud trend information. This kind of database can then be queried to more effectively write rules for processing and quickly react to large compromise events. Because time is of the essence, a solid analytics strategy can provide an early warning system to public and nonpublic data breaches, allowing mitigation strategies to be developed ahead of the curve.

Comprehensive Suites Emerging

Invoking a combination of system parameters, neural networks, recovery services and advanced analytics provides financial institutions with a comprehensive blanket of fraud protection. Obtaining and securing those resources, however, can be difficult, especially when looking for the convenience of one-stop shopping. One solution, FIS Secured from Fidelity National Information Services,

provides that blanket of comprehensive protection along with the convenience and efficiency of a single provider.

“While the largest financial institutions have spent millions to develop advanced fraud mitigation strategies, smaller issuers need the ability to take advantage of similar tools,” said Tony Ficarra, executive vice president for FIS’ e-business division. “Processors are responding by developing multipronged solutions to combat the most common types of fraud, while allowing institutions to focus on the most important aspect of their card programs, the customer relationship. FIS Secured was developed with the smaller issuer in mind based on specific feedback from our clients and provides smaller issuers with equal—if not better—comprehensive fraud protection than many of the larger, more fragmented solutions other institutions are pursuing.”

Increasingly, financial institutions are requesting a total fraud package of risk man-

agement tools encompassing prevention, investigation, challenge, recovery and analytics. FIS Secured includes these resources and even goes one step further by guaranteeing its services. Through this program, institutions have the ability to receive reimbursement for fraudulent transactions through the warranty component of the program. When comprehensive fraud protection comes with a guarantee, financial institutions have peace of mind that no other fraud solution can match. **ES**

Preston Faykus is senior vice president/fraud management at Fidelity National Information Services. Prior to joining FIS, he worked with Euronet Worldwide where he was in charge of new technologies for Europe, the Middle East and Africa. He started his career with DialogBank in Moscow by helping to create and build the bank's issuing and acquiring business.

DO YOU KNOW...

Where your bank's next best branching opportunity lies?

The demographic and competitive dynamics of your proposed site?

The financial impact of your branching decisions?

FIND OUT.

Our Branch Site Analysis service discusses the primary indicators, risks and alternatives, forecasts profitability and recommends whether to proceed with the project.

THE ART OF POSITIONING

bancography

BRANCH PRODUCT RESEARCH BRAND

VISIT WWW.BANCOGRAPHY.COM TO LEARN MORE
OR CONTACT US AT 205-252-6671 OR INFO@BANCOGRAPHY.COM