



A WHITE PAPER

Protecting Against Debit Card Fraud

Integrating Proactive Solutions to Effectively Mitigate Loss

by Preston Faykus


AURUM
TECHNOLOGY



The Debit Card industry is exploding in popularity while experiencing tremendous change. The effects of the recent settlement by the national card associations, the subsequent increases in personal identification number (PIN) interchange by the regional networks and the abundance of new types of stored value debit products will force many financial institutions to re-evaluate their pricing strategies and marketing approach as they continue to grow their debit card businesses.

More than ever, the pervasive use of debit cards is stimulating interest from groups and individuals to invent new ways to steal money from financial institutions and the consumers that bank with them.

In 2002, there were approximately 175 million Visa® and MasterCard® branded debit cards that generated nearly \$318 billion in purchases, according to a March 2003 Nilsson Report. The estimate that many fraud experts place on signature debit card fraud is on average approximately seven basis points, which means that the loss related to signature fraud alone was estimated to be \$222 million in 2002. Fortunately, many debit card issuers do not face significant losses but the risk of fraud for unprotected institutions is significantly greater than those institutions that employ comprehensive fraud prevention programs.

As debit card transactions continue to increase, so does the associated risk of

fraud. And as the proliferation of plastic cards continues to change the issuing landscape, the nature of fraud itself is changing. Debit card fraud is no longer strictly the result of lost or stolen cards. Today's thieves are generally more proactive, organized and sophisticated in their techniques. Areas of debit card fraud that are on the rise include cards that have been compromised by skimming or counterfeiting, cards not received in the mail, and account takeovers using false identities.

The implications for financial institutions are clear. Advanced, proactive fraud prevention solutions are necessary to effectively mitigate both fraud occurrences and losses. As fraud attempts rise and new types of fraud surface, financial institutions must be in a position to react quickly, leveraging existing mechanisms to protect both the institution and its customers or members.

As debit card transactions continue to increase, so does the associated risk of fraud.

continued on page 2

Fraud from All Fronts

In an increasingly wired world, the Internet simplifies and expedites the sharing and selling of data to criminals across the globe. Anyone with a Web browser and an Internet connection can learn valid addresses and phone numbers to use for stolen or counterfeit cards. As more advanced equipment becomes accessible to fraudsters and the cost of that equipment decreases, financial institutions are finding themselves attacked from all fronts — making effective fraud prevention programs even more critical.

With technological advances, today's fraudsters are implementing more sophisticated ways to compromise debit cards — methods that enable criminals to make fraudulent transactions without having the original plastic card in hand. In these instances, legitimate cardholders usually do not even realize their debit cards have been compromised and would therefore not report them lost or stolen.

While the majority of debit card fraud loss stems from signature-based transactions, PIN-based debit card transactions are not immune to fraud. The ABA reports that in 2001, PIN-based fraud cost banks nearly \$51 million — and the losses appear to be growing.

The increase in PIN-based fraud, and debit card fraud in general, can be attributed to a

large degree to the increasingly sophisticated equipment used by fraudsters. The most common methods involve bogus ATM or POS terminals using skimming devices, remote cameras, or keyboard overlays to record cardholder PINs. In most cases, cardholders are not aware that their card data has been compromised and copied.

Consequently, evaluating both signature-based and PIN-based transactions in a real-time mode has become necessary to combat fraud.

Tracking PIN-based transactions offers the added benefit of identifying the specific geographic location of individual cards at the time of the transaction. This feature helps institutions recognize fraudulent transactions in geographically diverse locations. For example, if a cardholder makes a PIN-based transaction at a gas station in Florida and a fraudster tries to conduct a signature-based transaction to purchase stereo equipment in Chicago within the hour, the geographic discrepancies set off an alert that a fraudulent transaction is likely in progress.

Today's fraudsters are implementing more sophisticated ways to compromise debit cards.



continued on page 3

Fraud Prevention: An Integrated Approach

Use of effective fraud prevention programs can reduce fraud levels to five basis points or lower (i.e. less than \$.05 per \$100 of purchase volume). These fraud prevention programs feature integrated cardholder and transaction data systems, combined with the expertise of an experienced fraud prevention team.

Current best practices integrate both core processing and EFT platforms with secure card activation channels, rules-based fraud prevention systems and sophisticated neural networks — all leveraged by trained fraud analysts who evaluate suspicious transactions and contact cardholders and update the data within the fraud prevention model when necessary. This integrated approach delivers timely, synchronized data that can help finan-

cial institutions mitigate the risk associated with the evolving nature of debit card fraud.

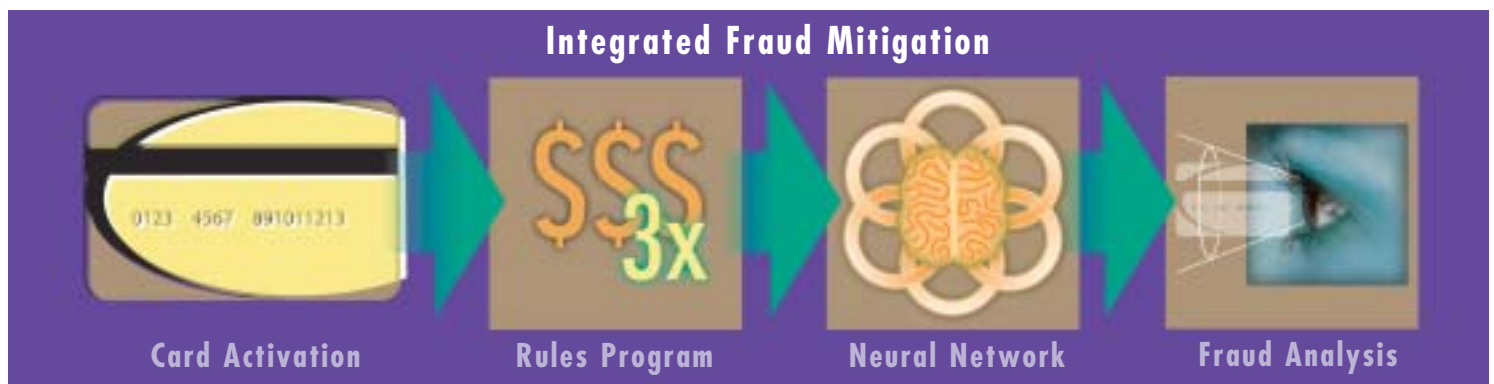
And since fraud management is an ongoing knowledge-based activity, integration across systems, as well as across functions, is needed to enable financial institutions to make the most of their fraud prevention programs. Through integration, each element of the solution works together to intervene before losses become significant. So as cases are investigated and actually confirmed to be fraudulent, the data within the fraud programs is updated to incorporate the new fraud patterns to help prevent future incidences.

Card Activation: Incorporating Secure Channels

Since a considerable amount of fraud still takes place as a result of cards being intercepted before reaching the intended

Through integration, each element of the fraud prevention solution works together to intervene before losses become significant.

continued on page 4



cardholder, card activation remains an important method to track newly issued cards. The use of audit mailers and convenient, yet highly secure card activation channels – such as ATM, telephone and Internet banking – are essential components of a comprehensive fraud prevention solution. By requiring cardholders to enter personal user information, financial institutions can mitigate potential fraud by ensuring that cardholders did indeed receive their cards before processing transactions.

Rules-Based Programs: Flagging Fraud Types

Most fraud prevention programs incorporate rules-based systems – solutions that model specific fraud occurrences – to evaluate current transaction patterns against typical fraud patterns in order to identify whether or not a transaction is fraudulent. Rules-based programs are used to identify common occurrences of fraud across groups of cardholders. These programs can also be written to address specific types of fraud identified by geographic regions, financial institutions or merchant types. For example, if the same

debit card number is used for two pay-at-the-pump transactions and a purchase at an electronics store within two or three hours, the suspicious sequence of transactions would cause the system to generate an alert and possibly even block the card as a result.

Rules are also needed to protect cardholders with very little transaction history since the rules themselves will identify fraudulent spending patterns. The key to developing a successful rules-based program is writing and implementing effective rules without adding superfluous parameters that may only result in slowing down the transaction evaluation process.

Neural Networks: Tracking Cardholder Behavior

Neural networks also play a critical role in fraud prevention programs. The strength of a neural network lies in pattern recognition and classification as well as in prediction and control of complex data patterns. In fact, a neural network is designed to “learn,” updating itself in

Use of effective fraud prevention programs can reduce fraud levels to five basis points or lower.



continued on page 5

similar fashion to a human brain. When used in the debit card industry, these sophisticated fraud prevention solutions store thousands of examples of valid purchase transactions and constantly update individual cardholder purchase information. Future purchases can then be evaluated against the most current data profile of each individual cardholder.

As authorization requests are processed, each transaction is evaluated based on the individual's debit card transaction history. The transaction is analyzed to assess the potential risk of fraud and scored so that high-risk transactions receive a corresponding high score. If the score exceeds one of the predefined thresholds, an alert is generated and sent to an experienced fraud analyst for further investigation.

Parameters typically used in neural networks include long-term purchase behavior, frequency of purchases, types of merchants that cardholders usually go to regularly, distance from home, and even the cardholders' most typical shopping days and times.

Fraud Analysts: The Human Touch

Since individual cardholders rarely fall into perfect spending patterns, it is important to incorporate the "human factor" for effective evaluation and resolution of suspicious transactions. Skilled fraud analysts and fraud prevention managers represent a crucial step in examining the results produced by rules-based and neural network fraud prevention systems.

When a neural network creates an alert for a suspicious transaction, fraud analysts are needed to assess those transactions and investigate whether the incidents are indeed fraudulent. Most effective fraud prevention initiatives will tightly integrate the fraud analysis and cardholder contact functions. This integration is key because both analytical and interviewing skills are necessary to effectively maintain a low level of fraud without alienating cardholders by bombarding them with constant transaction checks. One of the most critical roles that fraud analysts and fraud prevention managers play is integrating new rules and parameters into the fraud prevention systems to help reduce the risk of loss from future incidents.

It is important to incorporate the "human factor" for effective evaluation and resolution of suspicious transactions.

continued on page 6

Balancing Act

A balance must also be reached between the amount of cardholder contact that financial institutions feel comfortable with the number of potentially fraudulent transactions that may be missed. An institution could theoretically set its goal of acceptable fraud at a zero level, but at that level the institution will obviously not be maximizing its profit potential. Because at that level, the financial institution is most likely alienating its existing cardholder base by calling them for 98 percent of all transactions processed.

Proactive Resolution

An integrated fraud prevention program might also include a process for initiating chargebacks once fraudulent transactions have been confirmed. An effective process could streamline the amount of administration work involved, while expediting the process of obtaining the funds due to the financial institution. It is important to ensure that a single group controls the chargeback function so that all disputed items can be properly tracked and managed.

The Bottom Line

Debit cards are and will continue to be essential retail products for financial institutions. Financial institutions are well advised to take a proactive approach: Implement integrated fraud prevention solutions in order to protect both the institution and its customers or members. In today's ultra competitive environment where financial institutions are constantly looking for ways to bolster the bottom line, it is regrettable for financial institutions to experience significant fraud losses — losses that could have been prevented.

Combining fraud prevention practices with secure card activation, well-written rules-based systems, sophisticated neural networks tools, and highly trained fraud analysts can help ensure the profitability of debit card programs.



For more information:

To learn more about Aurum Technology and the open, integrated and comprehensive solutions we can deliver as you work to mitigate fraud loss, call us at 877.IT.AURUM (877-482-8786) or send an email to information@aurumtechnology.com. We look forward to being of service to you, your institution and, ultimately, your members.

About the Author:

Preston Faykus has a diverse international banking career that spans the continents of Europe, Asia, Africa and North America and more than a decade in the disciplines of product development, market strategy and retail banking. He has built eBanking programs from the ground up and currently serves as eBanking product manager for Aurum Technology, leading the company's ATM and EFT lines of business.

Aurum At A Glance

- ▶ More than 30 years of profitable growth through superior customer relationships
- ▶ Focuses entirely on community-based and mid-tier institutions – from de novos to \$25 billion in assets
- ▶ Employs 1,400 professionals at 36 locations, including 24 “Check 21-ready” image item processing centers
- ▶ Serves the retail and commercial needs of 1,200+ customers throughout North America
- ▶ Delivers integrated, open and scalable solutions comprising:
 - Core Solutions
 - eBanking
 - Check Imaging
 - Business Intelligence
 - Strategic Services
- ▶ Leverages best-of-breed solutions offered by leading industry partners
- ▶ Processes 8 million accounts and more than 1 billion items annually



www.aurumtechnology.com

