BEYOND EMV

PROTECTING YOUR FINANCIAL INSTITUTION AND CARDHOLDERS BY GETTING READY FOR WHAT'S NEXT NOW

fiserv.

WELCOME

Reliable fraud detection capabilities are the key to defending your financial institution and your credit, debit and prepaid cardholders from today's ever-evolving fraud hazards. With the implementation of the EMV standard aggressively underway within the U.S., significant strides are being made against fraud. But EMV is only a partial answer to the overall war against fraud since it will not mitigate "card not present" (CNP) fraud. And the full impact of that other au courant buzzword, tokenization, is years away.

To protect your institution and cardholders now, you still need sensible risk management approaches that complement the promise of EMV and tokenization with established best practices. These best practices include real-time transaction scoring that will block suspected fraudulent transactions, real-time case management and monitoring, and tracking and monitoring fraud alerts on compromised cards. You should also consider deploying specific authorization rules that fit the unique characteristics of your cardbase. Finally, you'll need empowered consumers who understand the importance of proactive management of their accounts and mobile card control applications that enable their involvement.

THE CHANGING LOOK OF FRAUD

In its earliest form, card fraud resulted primarily from stolen cards which FIs were able to combat through card activation processes and first-generation neural networks. But as new payments technologies proliferated, fraud also became more sophisticated and increased through large scale operations that included phishing, skimming, and data breaches. Enter EMV, which provides new safeguards during card present transactions.

Despite (and likely because of) the positive impact of EMV, a large percentage of new fraud is moving to CNP transactions (like ecommerce transactions) which EMV does not protect.

CURRENT FRAUD TRENDS INCLUDE:

- ✓ More diverse cardholder activity – making it more difficult to recognize cardholder patterns
- ✓ More creative and pervasive fraud, including flash fraud which can result in huge losses before issuers can react and respond
- ✓ Criminal attacks that have increased in magnitude via both local and global criminal organizations
- ✓ Social engineering tools that exploit consumers with phishing attacks that take advantage of cultural and current events
- ✓ Criminal efforts to install malware to obtain online credentials and any pieces of personal information
- ✓ Vishing/SMiShing.

The cost of payments fraud is soaring because new merchant and financial institution breaches are occurring with unsettling regularity. But the true cost of this fraud – already billions of dollars annually – may underrepresent the total cost to financial institutions. In addition to the actual fraud loss, there are additional categories of expense that are either underreported – or not reported at all:

- ✓ Operational expenses associated with research, cardholder service, and reissued cards
- ✓ The chance that newly issued cards will not be used or that accounts will be closed
- ✓ Overall profitability associated with cards and cardholders.

To remain protected, financial institutions must adopt a sensible approach that leverages industry initiatives like EMV and uses best practice tools. You'll also want to consider providing capabilities directly to your cardholders that empower and enable them to actively monitor and manage their accounts. This dual approach can make a true difference in the battle against fraud.

A SENSIBLE FRAUD FIGHTING APPROACH BEGINS WITH BEST PRACTICE TOOLS

Real-time transaction scoring, blocking suspected fraudulent transactions, real-time case management and monitoring, tracking and monitoring fraud alerts on compromised cards, as well as fraud rules that are specific to your cardbase, are essential ingredients to a successful risk mitigation strategy.

In fact, financial institutions that have begun reporting the results of using tools and services to combat CNP fraud – including the use of rule authorization tools that address unique business requirements – are performing significantly better than their peers. Fiserv, for example, expects to save its clients who leverage integrated and coordinated risk management solutions over $60 million in fraud losses each year, in the aggregate, for both CNP and card present transactions.

Although previously available tools were adequate for most types of fraud, FIs now need to invest in the latest technologies to protect their cardholders and their assets. FIs need to migrate from reactive to proactive and integrated measures, because fraud isn't slowing down.

NEURAL NETWORKS AND REAL-TIME DECISIONING

The most sensible starting point is the implementation of neural network capabilities that achieve a balance between aggressive fraud detection and serving cardholders: a strong neural network helps reduce fraud losses and focuses investigations on accounts and transactions that are most likely to be fraudulent.

Neural network technology builds cardholder profiles and utilizes predictive models to detect potentially fraudulent card usage. The predictive models are used to determine the fraud potential of each ATM and POS transaction by evaluating it against a complete history of cardholder usage patterns as well as unique transaction characteristics that are known to be fraudulent and legitimate. This process results in the recognition of any uncharacteristic transaction behavior. Transaction, industry, cardholder and merchant data are all used to forecast the likelihood of fraud.

With all neural networks, some level of false-positives will be generated. In a real-time environment, cardholders' transactions will be denied if the transaction score exceeds a defined scoring threshold. The lower the scoring threshold, the higher the false-positive rate and the more likely that legitimate transactions will be denied. Conversely, the higher a scoring threshold, the fewer actual fraudulent transactions you will prevent.

Real-time decisioning involves taking the neural network score into account in the authorization process. While the industry norm has historically been to review the neural network score after a transaction has already been approved or denied, there is increased interest in considering the likelihood of fraud (neural network score) in the transaction authorization process. Although this practice can drastically reduce fraud exposure, it can also have a negative impact on cardholders' ability to perform legitimate transactions and potentially impact overall card usage due to a higher rate of false-positives experienced with current technology.

Financial institutions should carefully weigh the level of risk they are willing to accept against the level of cardholder satisfaction they wish to deliver. An appropriate balance of the two is necessary to ensure you are protected against the majority of fraudulent transactions and that cardholders continue to view their cards as a safe and dependable payment method.

Inserting the neural network process into the authorization path provides more information upon which to make approve/deny decisions, enabling you to stop suspect transactions before they are approved. You will be able to select the criteria for those transactions you deem high risk that should be sent for real-time neural network processing (e.g. dollar amount, international, country codes, merchant category codes).

But even the most robust authorization systems can be enhanced. That's where a rule authoring capability becomes a differentiator. When you layer in rule authoring, you are ready to immediately address flash fraud – reducing fraud losses, maintaining consumer confidence and protecting the reputation of your institution. A robust rule authoring service will provide more availability to fields in the online message and greater flexibility in the number and complexity of rules that can be deployed, automating actions so risk mitigation can start immediately.

NEXT STEP: AUTHORIZATION LEVEL TRANSACTION BLOCKING

Transaction blocking gives you the ability to prevent the authorization of all transactions originating from countries or merchants known to generate fraudulent transactions. By taking advantage of the ability to override blocks at the card level, you can maximize your protection without inconveniencing your cardholders who may be traveling or working outside the United States.

The benefits include more precise fraud detection and increased fee income as you no longer unnecessarily block international card present transactions. According to industry statistics these transactions are an issuer's most profitable ones because the average value of an international card present transaction represents 175 basis points in value versus 16 basis points for a domestic transaction. These tools provide a method of blocking transactions you consider highly likely to be fraudulent by routinely denying the transactions in the authorization process. Issuers often look to Visa or MasterCard to implement blocks for specific countries. The associations' capabilities are adequate for blocking countries but they do not address other high-risk criteria such as merchant ID.

Issuers should take advantage of all available tools to mitigate risk. Transaction blocking capabilities are a key component of a sound risk management strategy and can be used to stop fraudulent transactions originating from specific countries, specific merchants and/or specific merchant types.

Your transaction blocking approach should provide you with the ability to place transaction blocks at the BIN and individual card levels. This approach enables you to block transactions you deem high risk, at your discretion.

Any combination of BIN and card level blocks should be set giving you the ability to override blocks for those specific cardholders who are traveling or working overseas. Blocking criteria should be set for all transactions or specific transactions —ATM, POS, eCommerce — within BIN and card levels. You assign the expiration date of each block to ensure compliance with card association rules regarding international/country blocking. Approve/deny options for each block include report and continue, deny, and deny and capture card. Daily and monthly reporting is important and block-related information should be incorporated into online transaction review screens, making it easy to manage your blocking strategies.

It is important to note that rules implemented for blocking transactions may only prevent the authorization of transactions through your processor's switch. Any transactions authorized through Visa and MasterCard during stand-in may require additional steps to implement blocks on the associations' systems. Additionally, blocking of transactions does not necessarily protect your chargeback rights.

NOW ADD COMPROMISED CARD TRACKING . . .

Industry trends indicate that blocking and reissuing cards each time a compromise occurs is not only expensive but also causes cardholder churn. Cardholders receiving reissued cards multiple times due to compromises, especially those that they may not have heard about in the news, frequently question the security of their issuing institution and a relatively high percentage will move their banking relationship to another institution. Although compromised cards are more likely to be used to conduct fraudulent transactions, taking this into account in the neural network process aids in stopping fraudulent transactions.

Visa and MasterCard provide alerts to you or your sponsoring institution when a data breach or card compromise event involving card data occurs. Issuers historically have routinely blocked and reissued cards to prevent losses.

Consider closely monitoring the activity on compromised cards and reissuing only those cards with suspicious or fraudulent transactions. Ensure your processor enables you to more closely scrutinize transactions for compromised cards in neural network processing.

. . . AND CASE TRACKING

A sensible case tracking tool will enable you to immediately serve any cardholder regarding cases that have been created or are being worked.

Case tracking tools put information online and at your fingertips so you have a complete repository of all actions taken on your cases and immediate access to updates and case statuses. Customized search options will enable you to view the information you need quickly and easily.

With an appropriate case tracking tool, you have real-time access to information and can:

- ✓ Search and download by case creation date, case status, card number, last name, tax ID, phone number, or city, state and postal code
- ✓ Download and review available transactions associated with a specific case
- ✓ Status cards and manage cardholder records optimizing back-office operations
- ✓ Determine a case status (Fraud, No Fraud, Unconfirmed)
- ✓ Directly enter actions or review actions already taken by your team, including:
    - Send a letter to the cardholder
    - Review case and cardholder demographic details
    - Dynamically select data to generate a custom report or print records.

Case tracking is made especially efficient through the use of transaction tagging – a feature that provides enhanced visibility to potential fraud trends. With tagging, transaction details – including the merchant, country and state – are already verified when you review cases, significantly streamlining the research process, resulting in quicker identification of fraud and expedited implementation of fraud prevention solutions.

RISK MANAGEMENT SERVICES

The risk mitigation needs of financial institutions are as varied as their asset sizes. When formulating a comprehensive strategy, you may want to consider customizable options – like risk management services – that complement your best practice toolset and provide additional insight and controls to assist in managing your fraud and risk management program.

Ideally, financial institutions can establish a one-to-one relationship with a member of their processor's risk analyst staff to assist in managing more complex and damaging fraud cases. This industry expert can provide advice on remediation strategies, design and implement fraud rules tuned to the unique characteristics of your cardbase, generate specialized reports, gather additional information, provide additional analytic services and supply other assistance to reduce your fraud exposure. This service allows financial institutions to augment their risk management program with highly seasoned and experienced risk analysts.

With risk management services, you receive insight and direction designed to address your institution's unique credit, debit and prepaid fraud risk exposure. The old adage is especially true here, "one size does not fit all," as it relates to fraud rules and strategies. As fraud evolves, these capabilities have never been more important. When fighting fraud, timing is critical – so a risk management service is designed to help you take swift action.

One obvious area a fraud risk analyst can assist you with involves strengthening card change authentication methods. Although you understandably want to provide your cardholders with flexibility to activate a card or make PIN changes at their convenience, you should first work with an analyst to understand the options and specific information you can use to authenticate cardholders. Your analyst can recommend the information needed beyond a social security number or date of birth. Understanding your options can help prevent fraud and provide a better and more secure cardholder experience. Once a cardholder is reliably authenticated, you can be assured your cardholders can safely use their cards at ATMs and the point of sale for purchases.

THE IMPORTANCE OF AN INFORMED AND AWARE CONSUMER

Cardholders who understand how to safely use their payment cards are reasserting themselves as one of the strongest lines of protection against card fraud.

Up-front cardholder education increases cardholder awareness which helps decrease unauthorized card use and fraud loss. Industry statistics show that cardholders who review their account activity on a routine basis are more likely to detect and report fraudulent activity, thereby reducing losses.

Implement a comprehensive cardholder awareness strategy that emphasizes protecting payment cards and account information from disclosure or risk exposure. Strategies can involve providing card usage instructions to cardholders as accounts are opened or sending statement stuffers and educational mailings. All cardholders should be made aware of:

- ✓ Safeguarding personal information and records
- ✓ Understanding their physical environment when using their cards—are people around who could pose a threat?
- ✓ Actively reviewing statements and receipts to ensure their records are accurate and that their card is not being used without their authorization
- ✓ Procedures for reporting lost, stolen or compromised cards.

THE PROMISE OF TOKENIZATION

The emergence of tokenization, which enables financial institutions to substitute their cardholders' personal account numbers (PANs) with a unique substitute value for use in the digital payments environment, shows how savvy consumers can aid financial institutions in the fight against fraud.

By choosing tokenized payments, consumers can simplify their purchasing experience by largely eliminating the need to enter and re-enter the card number when shopping on a smart phone, tablet, or PC. Payment tokens also help mitigate risk in the remote and proximity payments space by removing sensitive card information from the payment process.

Tokenization benefits include:

- ✓ Enhanced transaction efficiency
- ✓ Improved transaction security, allowing transactions to be signed and verified as originating from a specific device
- ✓ A secure method for third party enablement—e.g.: wallet, near field communication (NFC)
- ✓ Reduced risk of fraud in digital channels such as e-Commerce and m-Commerce.

EMVCo, the global standards organization that oversees EMV specifications, has expanded its scope to include tokenization specifications. The development of a global tokenization standard enables a new generation of payment products while maintaining compatibility with the existing payments infrastructure.

PUTTING CONTROL IN A CARDHOLDER'S HANDS

Aware consumers are also being empowered via new technology capabilities that will enable them to actively manage their card usage by defining when, where and how their payment cards are used. These services are ideal for cardholders who want to proactively manage their card accounts through their mobile devices. The financial management capabilities of these tools will enable cardholders to:

- ✓ Monitor and control card transactions
- ✓ Manage and review card usage for their dependents
- ✓ Enforce spending policy compliance for transactions on business cards.

Cardholders can simply download these applications to their mobile device then customize usage settings and alert preferences.

Mobile card control apps can report or restrict PIN and signature transactions performed by payment cards, enabling cardholders to manage, track, and report specific types of transactions and quickly detect unauthorized activity. Cardholders can generally customize their experience by choosing from a variety of options.

With card usage controls, spending limits can be established to allow transactions up to a certain dollar value and decline transactions when amounts exceed pre-defined thresholds. Transactions can also be monitored or controlled for specific merchant categories such as gas, hotel, travel, restaurants and groceries.

Card on/off settings are also invaluable. When the card is "on," transactions are allowed in accordance with the cardholder's usage control settings. When the card is "off," no purchases or withdrawals are approved until the card is subsequently turned back "on." This control can be used to disable a lost or stolen card.

Location controls can restrict transactions to merchants located within a certain range of the cardholder's location (using the phone's GPS); transactions requested outside of the specified range can be declined. Regional controls use city, state, country or zip code on an interactive map; transactions requested by merchants outside of a specific region can be declined.

Alerts can also be set up to inform cardholders of specific types of transactions. Generally, card control apps can send an alert when a card is used, when a transaction is approved and exceeds any of the permitted use policies, or when a card transaction has been attempted but is declined. The alert is sent in real time, immediately after the transaction has taken place or has been declined.

FINANCIAL INSTITUTION SUCCESS

Cards – debit, credit and prepaid – are the payment method of choice for U.S. consumers, but their fraudulent use won't stop just because you're not ready for it. Unfortunately, EMV is only a partial solution since it focuses on counterfeit fraud only. Every financial institution must still examine its other vulnerabilities, identify its unique needs, and determine an appropriate balance between investigating fraud and processing consumer transactions quickly and efficiently.

Incomplete fraud services will seriously imperil your success, so you must do everything you can to ensure the integrity of card account information. Rapidly identifying when fraud has occurred will advantageously position your financial institution.

To succeed, you'll need to build comprehensive and holistic fraud detection strategies that combine risk solutions with personal, hands-on investigative and support services and significant consumer empowerment and engagement. Comprehensive tools, rules, and strategies will provide you with prudent business practices you can use to highlight your commitment to risk management and cardholder satisfaction.

Today's fraud trends demand risk management strategies that improve detection and operational efficiency. An integrated and coordinated risk management solution enables you to build a seamless, multilayered defense against increasingly complex fraud scenarios.

ABOUT FISERV

Fiserv, Inc. (NASDAQ: FISV) is a leader in financial services technology and one of FORTUNE® magazine's World's Most Admired Companies. Fiserv enables clients to achieve best-in-class results by driving quality and innovation in payments, processing services, risk and compliance, customer and channel management, and business insights and optimization. For more information, visit www.fiserv.com.