“ASK THE EXPERTS: FRAUD MITIGATION STRATEGIES”
Webinar Q & A Session Responses

1. What are current fraud trends?

Fraud continues to be a growing problem. Current fraud trends include:

**E-commerce fraud:**

- Card-not-present (CNP) fraud is a popular form of fraud occurring online. A purchase can be made with just the card number; no physical card is needed.
- Friendly fraud is carried out by someone who places an order online and follows up with a complaint. The fraudster usually states that they never made the purchase or did not receive the merchandise.

**Foreign fraud** – International crimes rings strive to reach out to potential victims by phone, e-mail, postal mail, and through the Internet to try to trick them into sending money or giving out personal information in the form of fraudulent purchases from overseas companies/individuals, investment scams, the Nigerian letter scam, advance fee scheme and foreign exchange fraud, etc.

**Domestic fraud in stores** – Various types of fraud have been occurring in grocery stores, drug stores and department stores. For example, PIN pads have been tampered with, fake UPC labels have been used and employees copying checks are some of the schemes used to defraud stores.

**Vishing and SMishing:**

- Vishing is an unsolicited voice mail or mobile phone call in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. For example, the fraudster may state that they need to verify a card number or transaction because there is a problem with the card.
- SMishing is an unsolicited text message requesting a call back to a phantom phone number in an effort to get personal information.

**Mobile fraud** – Mobile Web sites are generally less protected; therefore, mobile phones are emerging as a new channel for fraud.

**ATM fraud** – Debit card numbers have been obtained by fraudsters from ATM skimming.

2. What are some best practices for detecting fraud?

Here are some best practices to protect your credit union from fraud:

- For ATM fraud, your credit union should visually check your ATMs for skimming devices and review data for unusual activity on a regular basis.
- For card-not-present, lost, stolen, mail theft, and account takeover fraud, your credit union can establish the following best practices: CVV/CVC matching, 24/7 Neural Network monitoring, real-time decision making, address verification, authorization name match and daily parameter controls.
- For protection against Web site for phishing schemes, implement good anti-virus software.
- To detect wire fraud, monitor transactions and when unusual transactions have been identified block and investigate the transaction further.

For additional best practices, read the [Fraud Prevention Issuer’s Best Practice Guide](#).
3. What are best practices for determining if you’re under "attack"?

- A credit union may be under attack if there is an increase in the case detail report.
- If the credit union receives an increase in fraud alerts, there may be a fraud or breach incident that may impact your cardholders.
- Advise cardholders to notify the credit union of any suspicious activity.

4. How do we minimize risk?

Credit unions can minimize risk by establishing daily parameter controls such as daily limits, country code blocks and merchant code blocks.

5. How do we educate our members about fraud?

Credit unions can educate their members by providing helpful fraud prevention tips through the Web site, articles can be written for newsletters and take-one flyers can be placed in your credit union lobby.

How can we educate our members on avoiding Internet fraud?

Credit unions can advise members to protect their passwords, credit card number and PINs. Credit unions can also suggest that members look for security symbols or lock on the check-out screen on e-commerce sites.

6. What tools are available?

Internal tools, such as daily report monitoring and reviewing the incident report for all fraud, chargebacks and disputes can help credit unions minimize risk.

By utilizing and optimizing processor tools and strategies, such as CVV/CVC matching, travel indicators, Neural Network 24/7 monitoring, real-time decisioning, name matching and controlled block strategies in addition to the internal tools can help credit unions have a comprehensive fraud mitigation program.

7. What are best practices for recovery strategies?

Credit unions can establish check fraud and collection procedures of what to do once a loss has occurred. Credit unions can also involve law enforcement and contact their legal counsel.

8. How do we reduce fraud loss and avoid costly write offs?

FIS Secured for Debit and Credit cards can protect credit unions against unrecoverable fraud losses over $50 per occurrence, thus reducing your liability.

How do we reduce our fraud liability?

Review and adjust your current parameters and controls settings by establishing daily limits –Velocity controls and spend limits, etc.

How do we limit liability on PIN-based transactions?

Credit unions can limit the liability on PIN-based transactions by reviewing transaction reports and note any unusual transaction amounts and establish a process for verification and validation of the transaction. Another way to limit the liability is to establish tiered daily limit structure based on the risk profile of the cardholder.

Credit unions should check ATMs (card slot and PIN pad) on a regular basis for anything that is not ordinary to guard against ATM skimming.
9. What is the best way to stop counterfeit cards?

Implement CVV/CVC matching, Neural Network 24/7 monitoring, real-time decision making, report monitoring, authorization name match, daily parameter controls to help prevent and detect counterfeit card transactions.

10. What are best practices for handling card-not-present transactions?

Implement the following tactics to help combat CNP fraud: CVV/CVC matching, Neural Network 24/7 monitoring, real-time decision making, report monitoring, authorization name match, daily parameter controls and expiration date match. Also, utilize Verify by Visa or MasterCard Secure Code as an added feature for the issuer and cardholder to verify the customer of the transaction.

What are best practices for blocking foreign transactions?

Credit unions can use daily parameter controls and country code blocks. If a credit union does not want to block a whole country, the credit union can allow certain merchant category codes (MCC) such as hotels, restaurants, hospitals and financial institutions to be processed and block other types of merchants such as jewelry stores.

11. Once a breach or compromise has been announced, what steps should we take to determine an appropriate course of action? How do we reduce exposure after fraud has already occurred?

The first step is to evaluate the situation (type, number of accounts, patterns) to determine your exposure. Next, your credit union may want to adjust the daily parameter controls, notify staff, fraud management groups such as the FTC and notify law enforcement.

COMPROMISE MANAGER™ is a secure browser-based tool used to help credit unions to effectively and efficiently manage compromised credit card accounts for both Visa® alerts and MasterCard® events. This tool helps to:

- Evaluate risk
- Selectively block accounts
- Reissue plastics
- Notify affected cardholders
- Enable targeted fraud monitoring

12. Will U.S. be moving toward chip cards anytime soon and do chip cards help prevent fraud?

Yes, chip cards are available in the United States now. Eventually, chip cards will be required for all transactions. FIS has chip card functionality available today. The problem is that there are not many merchants that accept or can read chip cards.

13. What is the best way to review data to look for test transactions and to determine if there is a fraud pattern that may hit the CU before it hits?

Many fraudsters are moving away from using test transactions to commit fraud. Credit unions should monitor the daily reports and look for recent fraud accounts and use that data to cross reference test transactions.

14. Do we have to disclose to our debit card holders if we intend to no longer allow any card-not-present transactions or any manually keyed in transactions?

You may need to consult with your legal counsel to determine your disclosure requirements.
15. What is FIS doing to prevent Fraud?
Answer: FIS offers a comprehensive fraud management program that includes: transaction monitoring, case management, fraud analytics, investigations and recovery.

*What is included in FIS Secured?*
FIS Secured maximizes the power of FIS’ neural network technology and leverages an expert team of fraud analysts to analyze fraud trends, member spending patterns and real-time authorization information to identify and prevent potential fraud before transactions are completed. With FIS Secured, you also have access to Compromise Manager.

**Merchant Questions and Answers**

**How can we combat fraud from unauthorized transactions pushed thru by merchants?**
When a merchant forces through a transaction, they lose or forfeit their charge back rights. The credit can also report that merchant to Visa (usfraudcontraol@visa.com) or MasterCard (fraudteam@mastercard.com). The credit union can use daily limit controls and merchant blocks if fraudulent transactions are pushed through.

**Can we process fraudulent transactions as chargebacks? Ex. When signature on card is obviously not the cardholders?**
Any transaction identified as fraud can be processed through the chargeback system for review.

**What steps are there to take in order to recover a loss when you are up against "no chargeback rights"?**
A credit union can check with its insurance bond carrier for any solutions.

CSCU is dedicated to putting our expertise to work for you by providing a comprehensive suite of products and services to help you prevent and attack to diminish your future risk exposure. For more information regarding CSCU fraud solutions, visit www.cscu.net/fraudtools.

**About CSCU**
Approximately 3,000 member credit unions trust CSCU with their credit and debit card portfolios. CSCU gives credit unions access to the latest industry trends, responsive service and complete card processing solutions. As the nation’s largest card processing association, CSCU is a trusted partner for insight, education and proven tools that grow and strengthen credit unions.