Security Innovations for the Changing Face of Fraud
INTRODUCTION

Fraud is everywhere—and multiplying. In fact, 17.6 million Americans (7 percent of all U.S. residents) fell victim to identity theft in 2014, according to the Bureau of Justice Statistics. Nilson reports that global card fraud increased by 20.6 percent in 2015, while card volume grew by only 7.3 percent. And JAVELIN research published on Creditcards.com projects that the total value of fraudulent card-not-present transactions alone will approach $19 billion in 2018.

As any credit union will attest, fighting fraud is like putting out a wildfire. It requires all hands on deck, a highly effective strategic plan, a powerful arsenal of tools, and a 24/7 commitment to success.

Toward that end, CO-OP Financial Services remains dedicated to delivering innovation on all fronts. Here is what we have learned about the state of fraud today—and about how credit unions can apply the most advanced security innovations toward the safety of their members.
CHAPTER 1: FALSE POSITIVES AND THEIR IMPACT ON REVENUE

When it comes to fraud detection, credit unions walk a fine line. Identifying fraud takes advanced computing systems and sophisticated algorithms designed to uncover anomalies in member spending patterns. However, not every anomaly equates to fraud. And declining a genuine transaction can break member confidence in your card products.

“False positives are a common, everyday issue,” said John Buzzard, CO-OP’s fraud expert. “Trying to avoid them is like reaching into a paper bag full of different colored marbles hoping to withdraw the same color each time. It’s a statistical impossibility.”

“For every incidence of fraud detected there are almost always a few suspects that end up being non-fraudulent transactions,” said Buzzard. “The important question to ask is whether the fraud captured is worth the number of false positives that result from the process.”

He adds that, as problematic as false positives are for credit unions, they can bring even greater frustration to the member involved. In fact, JAVELIN research reports that 39 percent of declined cardholders abandoned their card after being falsely declined.

“A declined transaction at the point of sale is not only a hassle for the cardholder—it can also be embarrassing,” said Buzzard.

A $118 Billion Problem
According to JAVELIN research, 15 percent of all cardholders have had at least one transaction incorrectly declined in the past year, costing issuers nearly $118 billion.
FALSE POSITIVES AND FRAUD PREVENTION
A Balancing Act for Credit Unions

False positives are a costly, time-consuming and aggravating byproduct of even the most effective fraud prevention strategies. However, there are best practices credit unions can embrace to limit their impact. Here is what you need to know:

FALSE POSITIVES COST ISSUERS BILLIONS
(Source: Javelin Strategy & Research)

15%
Of all cardholders have had at least one transaction incorrectly declined in the past year

$9B
By comparison, what actual fraud costs issuers annually

$118B
What these declines cost issuers nearly annually

39%
Of declined cardholders abandoned the card after being falsely declined

IMPACT ON E-COMMERCE
(Source: Businessinsider.com)

$8.6B
What U.S. e-commerce merchants will lose in falsely declined transactions in 2016

3 REASONS FOR FALSE DECLINES
(Source: Businessinsider.com)

1. Conflicting shipping and billing information
2. Differing risk appetites among issuers and merchant acquirers/processors
3. Outdated card information
FALSE POSITIVES AND FRAUD PREVENTION
A Balancing Act for Credit Unions (continued)

WAYS CREDIT UNIONS CAN CUT LOSSES

1. Rely on cutting-edge fraud prevention technology
   - Falcon Fraud Manager
   - FICO data analytics
   - Machine learning technology

2. Create more granular fraud strategy rules

3. Green light mildly suspicious transactions - then contact the cardholder to verify

4. Stay up to date on the latest fraud trends and prevention technologies

WAYS TO EMPOWER MEMBERS

1. Enable them to secure their own cards with mobile card controls and alerts

2. Educate members on fraud—and on the reality of false positives

3. Talk to them about the importance of travel notifications

4. Offer tokenized digital wallets—and promote their security

5. Communicate via two-way texting to alert members to potential fraud

We have never had to be more vigilant in our action around fraud containment. CO-OP will continue to invest in a strong blend of real-time analytics combined with a variety of tools that address problem areas like identify verification - always with a goal to balance between member service and fraud prevention.

Todd Clark, President/CEO, CO-OP Financial Services
A Constant Balancing Act

For activity that is mildly suspicious, Buzzard advises credit unions to forego declining the transaction and to instead contact the cardholder immediately after the purchase to verify its legitimacy. “These conversations need to be handled delicately,” he said. “While many members appreciate this outreach, others may view it as an inconvenience.”

To help reduce the incidence of false positives, Buzzard recommends adjusting fraud strategy rules so they are as detailed as possible. “Our risk escalation team works seven days a week to fine tune fraud strategy rules for our client credit unions, and is supported by a cutting-edge suite of fraud prevention tools, including the Falcon Fraud Manager in Real Time and the power of FICO data analytics,” he said.

According to CO-OP President/CEO Todd Clark, the company’s team consistently outperforms the industry in keeping false positives to a minimum.

“CO-OP’s false positive ratio is approximately 5:1, which means five cases are created for each incidence of confirmed fraud,” he said. “By comparison, the national average is 9–12:1. For fraud denied in real time, our false positive ratio is 1.3:1 versus a national average of 3:1.”

Todd Clark, President/CEO, CO-OP Financial Services

Emerging Tech: Machine Learning

To more accurately distinguish fraud from genuine transactions, financial industry leaders are looking to new advances in machine learning technology. According to the Washington Post, the Visa Advanced Authorization System employs machine learning and continues to advance its speed and accuracy to protect cardholders from both fraud and false positives.

MasterCard recently announced new Decision Intelligence Software, which analyzes hundreds of pieces of data related to a transaction instantaneously, as that transaction unfolds. The company is calling it “the first use of AI being implemented on a global scale directly on the MasterCard network.”

CO-OP’s 2017 technology roadmap also includes new, advanced machine learning technology, which will integrate with the Falcon Fraud Manager platform to create an even stronger scoring mechanism for detecting fraud.
CHAPTER 2: ARMING MEMBERS IN THE FIGHT AGAINST CARD FRAUD

To prevent card fraud, members may be a credit union’s most powerful resource. Ondot reports that financial institutions whose members use mobile apps for card controls and alerts reduce fraud by as much as 40 percent. According to Visa research cited by PYMNTS.com, merchant sites that accept their customers’ EMV cards nationwide have seen counterfeit fraud drop by 43 percent. And tokenized digital wallets, such as Apple, Samsung and Android Pay, are recognized by experts as virtually impossible to compromise.

While each of these innovations plays a unique role in protecting payments, all share a common thread—they place fraud prevention squarely in the hands of consumers.

Here’s why members should have them:

Battling Fraud with a Smartphone

Ultimately, only your members know how they are using their cards, which is why it makes sense to engage them in fraud prevention.

Mobile apps for card controls and alerts allow members to quickly and easily specify exactly when, how, where—and with which merchants—their cards can be used. For example, CO-OP’s CardNav app allows members to receive alerts whenever a card is utilized, with the ability to authorize or deny transactions before they are carried out. Users can set spending limits, authorize additional family members for usage, and even temporarily turn cards “off” when not in use. Members can also track important financial information ranging from account balances to payment due dates.

Why Act Now:

Effective October 14, 2016, for Visa, and April 21, 2017, for MasterCard, every U.S.-based card issuer must give cardholders the option to register for some basic alerts.

Moving beyond basic alerts, card control apps empower members to prevent fraud vs. just detecting fraud.

(Source: Ondot)

Protecting Cardholders at the Point of Sale

In more than 80 countries worldwide, EMV chip cards have virtually eradicated card-present fraud. The technology works by issuing a dynamic code for each transaction that is processed by the merchant. As a result, member account information remains securely out of a fraudster’s reach, locked behind the firewalls at the payments networks.

**EMV Inroads, According to Visa:**

- 388 million Visa EMV cards have been issued nationwide
- 1.7 million locations across the country are chip-enabled
- 40 billion chip-on-chip transactions have been processed (total volume)
- 41 percent of Visa’s in-store payment volume is chip-based today

(Source: PYMNTS.com)

Up Next—EMV 3DS 2.0

EMV 3-D Secure (3DS) 2.0 is a new specification that will allow consumers to authenticate themselves with issuers for card-not-present purchases or when verifying their identity for non-payment activities, like adding a payment card to a digital wallet.

(Source: Global Banking and Finance Review)
Digital Wallets Go Mainstream

While consumers and merchants have been slower to embrace digital wallets than many had predicted, this dynamic is changing. According to Macdaily.com, Apple Pay transactions were up 500 percent year-over-year in September 2016—with more Apple Pay transactions processed during the month than in all of fiscal 2015. As with EMV, tokenization protects member account data by transmitting a unique code—or token—for each transaction instead of the PAN, preventing actual cardholder data from ever changing hands.

Mobile Revolution

If the outlook for mobile is any indication, digital wallets have a bright future. For 2017, the number of U.S. smartphone users will reach an estimated 222.9 million, and the number of smartphone users worldwide will exceed two billion. (Source: Statista.com)

Before Members Pack Their Bags . . .

Make sure members know to file travel notifications with your credit union before leaving town. This step can save everyone involved time and aggravation, and ensure that members have full access to their cards while away.
CHAPTER 3: SHORING UP THE BACK OFFICE: THE POWER OF MACHINE LEARNING

Machine learning continues to make industry headlines as credit unions and other financial institutions increasingly find value in big data. According to a study completed by London-based Oakhall and published on finextra.com, global financial services firms could save $12 billion annually—or more—by optimizing adaptive, machine learning fraud management technology.

So what is machine learning and why is it so effective at catching card fraud?

In 1959, artificial intelligence pioneer Arthur Samuel defined machine learning as a “field of study that gives computers the ability to learn without being explicitly programmed.” It accomplishes this by employing advanced pattern recognition algorithms and computational learning theory to teach the computer, in essence, how to think.

As a fraud detection tool, machine learning enables highly accurate predictive analytics based on enormous volumes of complex—and ever-changing—data.

More Effective Than Humans

Research published by Mercator Advisory Group in conjunction with CO-OP states that, “In most situations where human beings determine risk today, a machine learning algorithm will be able to outperform those humans.”

Machine learning also outperforms the neural network technology widely used by financial institutions to detect card fraud.

“Neural networks follow a rules-based approach that requires a human to program the rules,” said Buzzard. “New advancements in machine learning technology now enable the system to intelligently develop its own criteria for what constitutes fraud, based on vast amounts of historical data in the system.”

He adds, “The technology is rapidly becoming mission critical because fraud has changed dramatically in 2016. We are now at the point where fraud has mutated and outpaced the general thoroughness of neural networks.”

The good news for credit unions, Mercator reports, is that third-party software suppliers have already invested heavily to integrate machine learning into their software, substantially reducing the cost and effort to employ the technology.
Beyond Fraud Detection

While machine learning shines in detecting fraud, there are other valuable credit union applications for the technology, including the following:

1. Cross-selling products
2. Facilitating member satisfaction scoring
3. Expediting diagnostics for technical support

A More Intelligent Member Profile

Machine learning makes a fraud detection system faster—and smarter. For example:

Machine Learning by the Numbers

IBM researchers working with a large U.S. bank reported that machine learning yielded a 15 percent increase in fraud detection, a 50 percent reduction in false alarms, and a total savings increase of 60 percent.

(Source: helpnetsecurity.com)
CHAPTER 4: WHY ATM SKIMMING IS RAMPANT (AND HOW TO STOP IT)

ATM skimming is increasing—exponentially. According to USA Today, FICO reported earlier this year that ATM skimming is prevalent across virtually every region of the U.S., and that it increased overall 546 percent year-over-year. And while most U.S. ATMs are in the process of migrating to fraud-resistant EMV technology, many are not there yet, making them particularly vulnerable to card fraud.

“Skimming is a huge issue this year,” said Buzzard. “As long as magstripe technology exists on payment cards, counterfeit skimming will continue.” According to Buzzard, ATMs have always been targeted by criminals. “Because ATMs require PINs to be used in tandem with a payment card, they are fertile hunting ground for fraudsters looking to capture both magstripe and PIN data from unwitting consumers,” he said.

With skimming devices evolving into sleeker, smaller and more authentic looking replicas of actual ATM components, detecting their presence is becoming increasingly difficult.

Periscope Skimmers—Tiny, But Mighty

“Financial institutions now have to look for miniscule devices known as ‘periscope skimmers’ that fraudsters install inside ATM magstripe readers, hidden from view,” said Buzzard.

According to PYMNTS.com, while periscope skimmers are small enough to evade detection, they can hold up to 32,000 credit card numbers, and sport a battery life of up to 14 days.

To mitigate the damages from periscope skimmers and other tools used to perpetrate ATM fraud, Buzzard advises credit unions to work closely with industry experts such as FICO’s Card Alert Service (CAS).

“CAS has been a leader in ATM skimming detection for decades and remains one of the best industry resources for managing losses from unauthorized ATM cash withdrawals,” he said. “Having physical security surrounding your ATMs is also critical, as are regular device inspections and member education.”

4 Security Precautions Every Member Should Take

1. Sign up for account alerts and two-way texting capabilities that expedite communication and confirmation of fraud
2. Transact only in environments they trust—If an ATM feels unsafe, members should move on to an alternative location where they feel safe
3. Check their financial accounts everyday to ensure funds are secure
4. Follow the adage “If you see something, say something”

“It is not uncommon for a consumer to discover a skimming device on an ATM before the financial institution has a chance to catch it”

John Buzzard, Strategic Technical Account Executive, CO-OP Financial Services
CHAPTER 5: EDUCATING EMPLOYEES AND MEMBERS - A CHECKLIST FOR CREDIT UNIONS

Fraud is damaging on many levels. In addition to the billions of dollars lost by financial institutions each year due to fraud, incidents can significantly impact member relationships and confidence in your card products.

Your employees and members need to know about fraud—and how to effectively protect against it. Follow our guidelines below for a more secure member base:

What Employees Need to Know . . .

About Fraud Trends
Employees need to be knowledgeable about all types of fraud, including the following:

- Social engineering fraud – A form of fraud that occurs when a criminal poses as a trustworthy organization for the purpose of soliciting information. Phishing is a good example of this.
- Card-based fraud – Theft or fraud committed using or involving a payment card, such as a credit or debit card, as a fraudulent source of funds in a transaction.
- Network-based fraud – Also called sniffing, this type of fraud uses computer software or hardware to intercept and log traffic passing over a computer network.
- Software-related fraud – Use of malicious software, such as spyware or Trojan Horse software, to secretly record user keystrokes, change security settings, and ultimately access accounts.

About Payments
All credit union employees should be well versed in the benefits of new, more secure payment technologies, ranging from EMV chip cards and tokenized digital wallets to MasterCard’s MasterPass, Visa Checkout, and smart phone apps for card controls and alerts. Branch employees and call center agents should be able to demonstrate each of these products to members and explain why they are secure.

About Communications
Credit union employees should exercise caution when disclosing information pertaining to internal fraud detection tactics. Fraudsters may be reading these documents, too, and may find the information helpful.

About ATM Security
Employees should understand how to monitor security across the credit union’s ATM fleet and how to conduct visual inspections in compliance with the Payment Card Industry Data Security Standards Council standards.
What Members Need to Know . . .

**About Security at Checkout**
Members should be equipped with a mobile app for card controls and alerts—and know how to use it. At the point of sale, they should know that chip-enabled and tokenized payments are more secure because they rely on encryption as a means of authentication.

**About Online and Mobile Safety**
Members should follow these rules whenever they transact digitally:

- Vary their login IDs and passwords
- Change login IDs frequently (every month or every quarter)
- Only download banking apps from trusted sources like the credit union website, and not from high risk web pages that appear in social media
- Utilize e-commerce solutions, such as Visa Checkout and MasterCard MasterPass
- Never purchase online—or by phone—from a retailer they don’t recognize
- Never click on a link embedded in an unsolicited email or pop up

Because fraud always thrives in an unprotected ecosystem, members also need to keep their antivirus and anti-malware software up to date on PC and Android platforms.

**About ATM Security**
Members should be instructed to only use machines in a safe, secure and well-lit area—and to pay close attention to their surroundings while there. Whenever a POS or ATM makes a member feel uneasy, it is always best to seek out an alternative to avoid risky situations.

**About Authentication**
Ease and efficiency don’t always equal security. Members should understand that the longer and more complex an authentication process is, the more secure it is.

The impact of fraud on credit unions and their members can be devastating - but information is powerful. An educated and vigilant credit union community is always a safer one.
CONCLUSION

As a credit union, protecting member assets is the most important service you provide. Your ability to shield members from the devastating effects of fraud speaks directly to your value proposition. By employing the most innovative technologies and strategies, and by staying informed on fraud tactics as they advance and evolve, you can deliver on your promise of security to members.

Making things inconvenient for fraudsters cannot mean making things inconvenient for members. Their experience must be both safe and seamless.

Todd Clark, President/CEO, CO-OP Financial Services

Find out about how you can empower your members with the latest security innovations from CO-OP. Visit CO-OPfs.org, email sales@CO-OPfs.org or call 800.782.9042, option 2