Standing Up to Fraud
How Credit Unions Mitigate the Threat Landscape

Credit Union Times
Natasha Chilingerian
Managing Editor
Standing Up to Fraud: How Credit Unions Mitigate the Threat Landscape

Introduction

In 2015, fraud led to 11 of the nation’s 16 small credit union closures. Fraudulent online transactions will reach $25.6 billion by 2020, up from $10.7 billion last year, according to Juniper Research. Distributed denial of service attacks rose by 15% from the fourth quarter of 2015 to the first quarter of 2016 in the financial sector, a Verisign report stated. And the Identity Theft Resource Center revealed as of May 24, 2016, a total of 420 data breaches have occurred this year, up 22.1% over last year’s record pace for the same time period (344).

Those are just a few of the staggering statistics reported by CU Times this year that demonstrate just how dire a threat fraud is to the financial services industry – including credit unions.

We know mitigating these threats is top-of-mind for executives at credit unions of all sizes, and to learn precisely what they’re doing to keep their data and other assets out of thieves’ hands, we asked readers to complete an online survey.

In this whitepaper, you’ll find the results of that survey, as well as reactions and insights from industry experts. We hope it allows you to benchmark your fraud mitigation efforts against your peers and implement new strategies that will keep your institution – and your members’ data – safer than ever.

And, be sure to mark your calendar for Oct. 11 and 12, when CU Times will take a deeper dive into fraud prevention at its inaugural conference, “Fraud: Don’t Let it Happen to Your Credit Union!” at the Sheraton Dallas.

Who Was Surveyed

CU Times’ 41-question fraud survey ran online from May 10 to 18, 2016 and drew 141 respondents. Of those respondents, 38.3% work at credit unions with assets totaling more than $750 million. Twenty-seven respondents, or 19.15%, serve at credit unions with $250 million to
$749.9 million in assets, and the remaining respondents fall equally into three lower-asset tiers: 14.18% work at credit unions with $100 million to $249.9 million in assets, 14.18% at $50 million- to $99.9 million-asset institutions, and the same percentage at institutions with less than $49.9 million in assets.

When asked to select their role at their credit union, the most respondents (42.55%, or 60) chose “other, not IT related.” “C-suite, not IT related” was selected by 27.66% and 20.57%, or 29, said they were a credit union SVP or vice president, but not in an IT capacity. Smaller numbers of respondents selected “C-suite, IT related” (6.38%, or nine), “SVP/VP, IT related” (2.13%, or three) and “other, IT related” (0.71%, or one).

**Fears and Real-Life Experiences**

There’s no question that the constantly looming threats of fraud have credit union executives worried. And it’s not just one type of fraud that’s raising their blood pressure – when asked about the specific areas that scare them the most, nearly every respondent selected multiple categories out of the seven provided.

Topping the list were cybersecurity (63.5%), risks beyond your control (retailers) (58.39%), member understanding of risks (48.18%) and compliance requirements (44.53%).

Fears stretched beyond the categories provided in the survey as well – when asked to list other areas of concern, responses included cloud security, phone and cross-channel fraud, ATM skimming and elder financial abuse.

For many executives, these fears have been justified by fraud experiences at their own institution. Eighty-seven percent of respondents said their credit union had been affected by fraud, while a little less than 11% said theirs had not and 2.13% said they didn’t know if it had been hit.

Of those who had experienced fraud at their credit union, a significant majority of respondents (70.54%) said the fraud originated at a merchant location.

Nearly 43% said it took place at their credit union, 32.14% said it began at their payments processor, 19.64% said it happened at another financial institution and 7.14% said they didn’t know where it occurred.

Fraudulent credit and debit card use was the most common culprit of fraud at credit
unions, with 85.71% of respondents selecting it as the reason behind the fraud they experienced. Data breaches ranked second (58.1%), followed by internal fraud and member error (both 16.19%), counterfeit currency (13.33%) and employee error (12.38%).

“The survey results are not surprising,” Terry Pierce, senior product manager for the Rancho Cucamonga, Calif.-based CO-OP Financial Services, said. “We are seeing the continuing increase of fraud due to data breaches, ATM skimming and card compromises. In addition, we are starting to see an increase in account takeover fraud.”

Other types of fraud reported by survey respondents included member scams, wire fraud and straw-buyer fraud rings. One respondent explained their fraud incident began in the call center, when a caller pretended to be several different members and relayed their personal information, managing to execute an account takeover.

Call centers are a growing fraud target. As CU Times reported in a Nov. 10, 2015 article, “The Next Fraud Frontier: Call Centers,” the Atlanta-based identity technology firm IDology found a jump in call center fraud from 2014 to 2015, fueled by a predicted post-EMV outbreak of card-not-present fraud.

“One interesting development in this year’s results is the rise in organizations reporting suspected call center fraud attempts — from 2% in 2014 to 13% in 2015,” the firm said.

How Credit Unions Fight Fraud … and What it Costs Them

Fraud is not an area where credit union executives like to see their dollars go, but protecting and recovering valuable data is a necessity, so there is little choice.

Fortunately, credit union professionals (37.5%) reported their total 2015 fraud expenses (including new technology and systems, card reissuance and member credit monitoring) equaled less than $100,000.

Nearly 19% said they didn’t know their total 2015 fraud tab, 23.21% reported spending between $100,000 and $249,999, 16.07% spent between $250,000 and $999,999, and 7.14% of
respondents said their fraud expenditures exceeded $1 million.

Executives said they expect their fraud expenses to be similar over the coming year, with nearly 34% planning to spend less than $100,000 and 26% expecting to spend between $100,000 and $249,999. A small portion (4.35%) expect to spend more than $1 million.

Of course, lowering fraud costs begins with prevention. Internal controls are the top tactic credit unions employ to prevent fraud (40.37%), followed by strong cybersecurity measures (22.94%), data and analytics (20.18%), employee training (13.76%) and member education (2.75%). Nearly 12% noted they utilize all of the above strategies.

A majority of respondents (almost 87%) said their credit union has implemented a mixture of internal and external fraud prevention resources. And to prevent fraud, credit union employees are willing to put in the time – 26.55% of respondents said employees dedicate more than 2,000 hours to fraud prevention, compliance and response annually.

However, not all credit union executives are confident their fraud prevention strategy is working. Only 11.4% of respondents called their strategy 99% effective, while a majority (58.77%) said it was 75% effective. Just 4.39% view it as less than 50% effective.

Steve Ruwe, chief risk officer for the St. Petersburg, Fla.-based PSCU, said he recommends credit unions spend more resources on member education.

“Credit unions are very focused on this and do a good job of addressing fraud on a number of levels, but I was surprised to see member education as low as it was,” Ruwe said after reviewing the survey results. “We believe involving the member
in fraud prevention can be a successful strategy for credit unions. There are tools out there, such as alerts and controls they can put on their card, which at an industry level are being underutilized and can help them prevent fraud.”

CO-OP’s Pierce agreed, stating that member awareness and education are key to preventing fraud.

“Members should be aware of fraud trends such as phishing schemes and fraud resulting from computer viruses and malware,” she said. “Members also need to be alert to when an ATM looks suspicious and educated on what to look for in terms of skimming devices and other forms of ATM tampering.”

She also recommended credit unions follow PCI DSS best practices, and ensure operating systems are hardened and kept up to date with patches.

One way credit unions can prepare for fraud costs is by purchasing a cybersecurity insurance plan. This strategy appears to be popular – 63.16% of respondents said their credit union carries cybersecurity insurance. Of those who don’t, a portion (15.15%) said the costs of insurance outweigh the anticipated risk.

In the Aug. 12, 2015, article “Cyberliability Insurance Grows,” CU Times reported the market for this insurance category is booming, as it recently posted a 36.6% compounded annual growth rate, according to recent data from ABI Research. However, experts warned credit unions often don’t understand what they’re buying when they purchase cyberliability insurance and fail to shop around, which can result in lower than expected payouts, higher than necessary premiums, and unpaid or underpaid claims. They recommended all credit unions considering cyberliability insurance have a lawyer review the policy before signing on the dotted line.

**Using Technology to Fight Fraud**

When it comes to fraud protection, technology has the power to either keep sensitive data out of the wrong hands or inadvertently leak information, which can lead to detrimental results. According to CU Times’ survey, many credit unions may be putting their member data at risk – 83.04% of respondents said their computers that access member data also access the internet and 10.71% said some of their computers that access member data also access the internet.
Only 2.68% said their computers that access member data don’t access the internet, and 3.57% said they weren’t sure.

Pierce said this poses a huge risk for credit unions.

“The key thing is insuring your network isn’t easily available, and if it is, you need to build a network of firewalls to ensure it’s secure,” she said. “The internet is pretty scary – once your system is open to the internet, anyone can go in there and attack. That’s what happening with a lot of the hacks. The hacker is finding a back door into the system.”

However, most credit unions appear to be diligent about detecting unauthorized, potentially malicious downloads. Slightly more than 68% of respondents said their credit union can detect unauthorized downloads via USB device or remotely, while 7% said it couldn’t and about 24% said they weren’t sure.

Using technology to implement effective security controls is key for credit unions looking to overcome fraud. In the June 1, 2016, article “Using Technology to Stop Internal Data Misuse,” CU Times reported organization insiders often misuse data – whether accidentally or intentionally – allowing hackers to infiltrate security defenses, leading to data breaches, malware intrusions, hardware and software misuse, and other costly incidents.

To adequately protect their data, credit unions must be aggressive about implementing and enforcing controls within their technological infrastructure, the article said. This includes limiting data access privileges, adding protection layers such as anti-spam systems to filter out phishing emails and scanning attachments for malware at the server level, and implementing anti-virus and data loss and leakage prevention systems to keep corporate data secure on all desktops and laptops.

Debit and Credit Card Fraud

While high-profile merchant card data breaches – from Target to Home Depot to Wendy’s – have dominated the news over the past few years, not as many credit union-issued debit and credit cards
are being compromised as one might think, according to *CU Times’* survey.

Seventy-two percent of respondents reported 49% or less of their credit union’s credit and debit cards had one fraud event in the last year. Debit cards appear to be a slightly bigger target for fraudsters – 9% of respondents said more than 50% of their debit cards had one fraud event in the last year, while only 3% of respondents said more than 50% of their credit cards had one fraud event in the last year.

Very few credit unions are immune to debit and credit card fraud entirely. Only 1% of respondents said they had not experienced any debit or credit card fraud events in the past year.

Ruwe said fighting debit and credit card fraud starts with focusing on data security in the credit union’s environment.

“I believe they are [focused on that], but that’s something they cannot pay enough attention to,” he said. “They must focus on hardening their environment.”

**Fraud and the EMV Shift**

The EMV liability shift occurred on Oct. 1, 2015, but many credit unions still have work to do when it comes to completing the transition. Thirty-eight percent of respondents said 49% or fewer of their credit cards are EMV compliant, while 36% said 50% or more of their credit cards are. Another 10% said they are not working on credit EMV compliance.

Fifty-eight percent of respondents said 49% or fewer of their debit cards are EMV compliant, while only 19% said 50% or more of their debit cards are EMV compliant. And 15% of respondents said their credit union isn’t working on debit EMV compliance at all.

Ruwe emphasized the importance of moving forward with both credit and debit EMV compliance.

“If you’re not working on it at all, that would surprise me, and I would question why you would think that’s a good plan,” he said. “But if you’re not completely done [with the transition], that wouldn’t surprise me.”

Many credit unions are not clear on their total EMV-related costs, according to the survey, but most said they haven’t devoted – or won’t devote – an exceptionally large chunk of their budgets to it.
About 30% of respondents said they spent less than $50,000 on EMV compliance in the past year, 28.16% didn’t know how much they spent, 19.42% spent between $50,001 and $100,000, 9.71% spent between $100,001 and $300,000, and just 4.85% said the cost totaled more than $300,000.

Similarly, 37.62% of respondents said they plan to spend less than $50,000 on EMV implementation in the coming year, 22.77% said they didn’t know how much they plan to spend, 18.81% are planning to fork out $50,001 to $100,000, 12.87% expect to spend between $100,001 and $300,000, and 4.95% plan on a tally higher than $300,000.

Reducing card fraud is a top motive for the EMV transition, but a majority of survey respondents – 65.05% – said it’s too early to tell if EMV compliance has lowered their fraud costs. Ruwe, however, noted PSCU’s research has indicated a reduction in fraud post-EMV.

“I’m seeing EMV as having a positive effect on reducing counterfeit activity,” he said.

Pierce added, “EMV implementation will reduce fraud for card present transactions, such as those performed at POS and ATM locations. However, the industry will need to be on guard as fraud is likely to shift from card-present to card-not-present transactions, such as online and mobile purchases.”

Survey respondents confirmed Pierce’s warning, with 53.92% stating their credit union has experienced a spike in card-not-present fraud. In addition, in the April 20, 2016, article, “Card Not Present Fraud Swells 11%: Study,” CU Times reported fraud attacks on U.S. online merchants rose 11% after the Oct. 1, 2015, EMV liability shift, according to the latest Global Fraud Attack. Overall, online fraud attacks (both successful and unsuccessful) spiked 215% for all of 2015, which translated to 27 fraud attacks for every 1,000 online transactions at the end of 2015 compared to only nine per 1,000 at the beginning of 2015, the article said.
ATM Fraud

Credit union ATMs are prime targets for criminals, who slyly place skimming devices on the machines and capture unsuspecting members’ card information. According to ATM company NCR, skimming accounts for global losses that exceed $3 billion annually and is a growing problem for credit unions in the U.S., CU Times reported in the April 2, 2016, article “SAFE CU Fights Skimming.”

However, a majority of survey respondents (67.35%) reported their credit union had not been affected by ATM skimmers in the last 12 months; 18.37% said theirs had been hit.

About 5% said their credit union didn’t operate ATMs, and 9.18% said they weren’t sure if they had been hit by skimmers.

Physical ATM inspection is a key defense against ATM fraud. A little more than 31% of respondents said their credit union inspects ATMs daily, 12.12% said they inspect their ATMs three to four times per week, 20.2% perform weekly inspections and 14.14% said they perform monthly inspections.

Three percent said they never inspect their ATMs, 11.11% said they weren’t sure, and 8.08% said they didn’t operate ATMs.

“To prevent ATM skimming, ATM operators must consider all points where card data may be accessible, in addition to the traditional point of vulnerability at the card entry bezel,” Pierce pointed out. “Credit unions with ATMs need to conduct frequent visual inspections of the ATMs and external connections. They should contact law enforcement immediately to report a fraudulent device. ATMs at most risk are ATMs where the network communications cable is located in a publicly accessible location.”

After enduring a number of ATM skimming hits in 2015, the $2.3 billion, Folsom, Calif.-based SAFE Credit Union implemented a combination of defenses.

It protected the computer inside each ATM with a firewall, virus protection and patching; installed cameras and alarms on each ATM; added PIN shield and cash trap inhibitors to the machines; and utilized NCR’s anti-skimming solution SPS (in which a bezel is placed over the existing card reader) in addition to performing regular ATM inspections.

Since then, the credit union said it has detected and thwarted skimming without affecting members.
Another ATM skimming defense is also a looming task on many credit union executives’ to-do lists: Ensuring all ATMs are EMV chip card-compatible. The EMV liability shift deadline for ATMs is Oct. 1, 2016, for MasterCard-branded credit and debit cards; Visa’s deadline is Oct. 1, 2017.

In the April 24, 2016, *CU Times* article, “ATM EMV Deadline Looms,” several experts said as credit unions continue to migrate their mag stripe plastic to chip cards, they should not neglect the impending ATM EMV deadline, and must prepare to educate members on the new ATM technology and emphasize chip card benefits. They also noted while there is no mandate for the ATM transition, the threat of fraud might be enough, as skimmers have been attacking older ATMs in final efforts to gather card information from the weakest points of the ATM network.

Most credit unions appear to be on board with the transition, according to the survey. Nearly 69% of respondents said they plan to upgrade their ATMs to comply with the MasterCard liability shift, 8.08% said they don’t, 15.15% said they weren’t sure and 8.08% said their credit union didn’t operate ATMs.

### Internal Fraud Controls

Fraud caused 11 of the 16 small credit union closures in 2015, leading to more than $12.5 million in NCUSIF losses, according to the NCUA, in addition to job losses and reputational damage to the credit union community nationwide.

*CU Times* reported those facts in the June 1, 2016, article, “Mitigating Internal Fraud at Small Credit Unions,” and survey respondents appear to be aware of internal fraud-related risks, as many said their credit union has implemented and enforced internal controls to prevent fraud.

Nearly 59% said their internal controls were adequate and 37.11% said they were somewhat adequate, most respondents said employees are trained annually (46.94%) or quarterly (31.63%) on internal fraud controls, and a majority said their supervisory committee reviews internal controls quarterly or annually (38.14% and 34.02%, respectively).
In addition, a large majority of respondents (74.23%) said they have an internal point person at their credit union responsible for ensuring internal controls are implemented correctly, and more than half of respondents (55.1%) said they continuously review internal control processes and take steps to improve them.

However, when asked if their credit union dedicates enough resources to internal controls, respondents were less confident. Nearly 36% said yes, 31.63% said maybe, 23.47% said no and 9.18% said they weren’t sure.

At the $344 million, Fairfax, Va.-based Fairfax County Federal Credit Union, addressing the human component through training and frequent, ongoing communication via multiple delivery methods has served as an effective internal fraud control strategy, according to Vice President – Compliance, IT and Facilities Nicole Bowen, who will appear as a speaker at CU Times’ fraud conference in October. The credit union also incorporates interactive, visual and auditory communications for employees to ensure it covers all the learning styles of its staff, she said.

Bowen also pointed out that technology controls may be useless if they work against the daily business processes a credit union has in place. She explained, for example, that an institution might implement a technology-based control that prevents a single user from signing in to multiple workstations.

What types of internal fraud controls should credit unions implement? Experts David Legge, president/CEO of the Legge Group in Manassas, Va., Joette Colletts, a senior manager in business protection risk management for CUNA Mutual Group in Madison, Wis. and Mike Sacher, CFO for the $947 million Xceed Financial Credit Union in El Segundo, Calif., offered the following:

- Regularly review employee accounts and the accounts of their relatives for any suspicious transactions.
- Have supervisors, auditors and/or supervisory committee members conduct counts of cash items at least on a quarterly basis.
- Separate loan approval from disbursement responsibilities.
- Ask an employee who does not have transaction authority to regularly review the credit union’s file maintenance transaction report to look for red flag transactions.
- Enable employees to anonymously report suspicious activity, such as with a post office box controlled by the supervisory committee, and/or offer a financial reward for employees who report internal fraud or abuse.
- Require all employees to take at least one week of vacation every year.
- Have a written fraud policy document that every employee is required to read and sign every year.
But, in this institution’s retail branches, employees often function in a universal role, serving members on both the platform and teller line throughout the day. Since these employees are committed to providing fast, efficient service for members, they see the control as an impediment to that goal.

Not understanding the reasons for the control, they may seek a solution to this new problem, and will continue to share workstations to avoid the hassle of signing in and out each time they move to a new location.

“In this example, our security control has now created a security vulnerability,” Bowen said. “Taking time to understand how each area of your organization operates as well as the challenges they may be facing relative to your security controls is a key practice in preventing security incidents and fraud.”

Communications and Fraud Events

Most credit union executives recognize the importance of effectively communicating with members and the media after a fraud event to mitigate damages and reduce reputational risk, according to the survey.

Nearly 76% of respondents said they have a comprehensive communications plan in place following a fraud event, and 60.64% have a comprehensive public relations plan in place following a fraud event.

In the Nov. 14, 2014, CU Times article, “Breach Prep Should Include Rehearsal: Onsite Coverage,” LT Public Relations President Casey Boggs said perfecting a communications plan before a cyberattack occurs is critical.

“Go through a dress rehearsal, go through the communication strategy and what you’re going to do,” Boggs said to attendees of the 2014 NASCUS/CUNA Credit Union Cybersecurity Symposium.

Steps a credit union should take in advance include improving its disaster recovery plan with communications support, developing a computer security incident response plan, establishing an emergency task force and identifying a spokesperson, Boggs said.

He added the spokesperson doesn’t always have to grant interviews to the press during a crisis and can deliver statements via email or phone instead.
As soon as a breach occurs, Boggs said credit unions must notify regulatory agencies and their members immediately. He also noted Twitter is a great tool for providing updates to members about the situation, while Facebook is best for reputation management.

“Concise, unified messaging across all mediums [is key],” Boggs said.

The Big Picture: Fraud-Related Risks

Fraud events can damage credit unions in a number of ways. When CU Times asked readers which types of risk are the most detrimental following a fraud event – financial, reputational, regulatory or operational – reputational and financial ranked the highest, with 48.86% and 30.34%, respectively. Next came operational with 10.11% of respondents ranking it as the highest risk category, followed by regulatory with 5.81% placing the category at the top.

“It doesn’t surprise me that they rate reputational as the highest, because credit unions have a strong relationship with their members,” Ruwe said in reaction to the results.

While credit unions surely suffer when a fraud event hits, the prevention process can also be costly in many ways, as Bowen pointed out. As the threat landscape rapidly changes, implementing an effective prevention strategy can be both time consuming and expensive.

“Financial institutions are not as nimble as the criminals,” she said. “Credit unions may find themselves more vulnerable as they wait for future enhancements to protect against the fraud techniques of today.”

And given the wealth of personal information that credit union members and employees can share on social media, fraudsters can easily find useful data for executing successful social engineering attacks, she said.

“These attacks are predicated on the fact that people are generally not great at protecting their personal data and are often unaware of the true danger of not doing so,” she said. “This presents significant risk to financial institutions.”

Conclusion

As fraud threats continue to grow and morph by the day, credit unions can’t afford to place an effective prevention strategy on the back burner. Fraud can occur anywhere within the organization — even call center fraud is on the rise.

Credit union executives said they expect to spend as much money on fraud this year as they did in 2015, purchasing and upgrading systems, reissuing cards and providing services to members like credit mon-
itoring. What can credit unions do to prevent fraud? Provide more education to employees and especially members.

Purchasing cybersecurity insurance is another strategy, but credit unions must ensure they understand what they are purchasing and shop around, so they can avoid inflated premiums and unpaid or underpaid claims. In fact, credit unions should have a lawyer review a cyberliability policy before purchasing it.

A credit union must also ensure its network isn’t easily available, and if it is, a network of firewalls must be created to bolster security. In fact, many hackers are using exposed back doors to access credit union systems.

Credit unions must also reinforce their security controls, because within the organization, insiders often misuse data, leading to data breaches, malware intrusions and other costly incidents.

To adequately protect data, credit unions must implement and enforce controls within their technological infrastructure by limiting data access privileges, adding protection layers such as anti-spam systems and implementing anti-virus and data loss and leakage prevention systems.

Even though they’ve made progress, credit unions still have work to do when it comes to EMV implementation. EMV is reducing counterfeit card fraud, but credit unions must now shift their focus to card-not-present transactions, such as online and mobile purchases.

Frequent physical ATM inspection is a key defense against ATM fraud, and operators must consider all points where card data may be accessible. ATMs at most risk locate the network communications cable in a publicly accessible location.

Internal fraud risk can be reduced by addressing the human component through training and frequent, ongoing communication via multiple delivery methods. Technology controls may be useless if they work against daily business processes. For example, a technology-based control that prevents a single user from signing in to multiple workstations could be over-ridden by busy branch employees who may share workstations to save time.

Finally, credit unions must develop both communications and public relations fraud crisis plans.

When fraud threats are at bay, credit unions can focus on more positive goals – growth, giving back to communities and helping members live their best financial lives.

To register for CU Times’ fraud conference, slated for Oct. 11 and 12 in Dallas, call 212-457-9510 or email fwolson@alm.com.

---

**Key Takeaways**

- Educate members.
- Protect networks from back door access.
- Implement and enforce technology and internal controls.