Top Ten Fraud Trends of 2011:

CNP Fraud and Skimming Continue to Afflict Credit Unions, but New Threats Surface on the Horizon

cscu
Building relationships. Strengthening credit unions.

Javelin Strategy & Research

Syndicated Research
Custom Research
Strategic Consulting

April 2011

Introduction

Fraud strategies at credit unions have required some revamping in recent times, due to a newly evolving fraud landscape and slowly recovering economy. If the big banks are aggressively driving away fraudsters, the fraud departments of credit unions might expect to deal with fraud in increasing volumes. With fraudsters always on the move toward paths of least resistance, credit unions could expect rising attacks as criminals strive to skirt around the tougher fraud controls put forth by larger institutions.

There were several large-scale fraud incidents this past year, ranging from ATM skimming rings to targeted phishing schemes. The Heartland data breach also continues to be on the mind of many credit unions. Card-not-present fraud has fast become a leading concern for financial Institutions of all sizes, and on an increasing level for credit unions, as online fraud is the easiest for criminals to perpetrate. When notifying members of fraud on their accounts, there's always the concern that a member will feel inconvenienced and believe that the credit union is not doing enough to protect them. On the flip side, credit unions are at an advantage in comparison to larger financial institutions, in terms of knowing their member base well and maintaining strong member relationships. In 2011, credit unions will rebalance their management of risk and fraud, particularly as card issuance continues to be lucrative for credit unions.

This whitepaper will cover the latest fraud trends affecting credit unions, and provide recommendations on how to best address the recent and emerging developments in fraud.

Top Ten Trends Impacting Credit Unions in 2011

The banking industry has experienced tremendous changes in the legislative arena this the past year, with Durbin and Dodd-Frank, just to name a few. Likewise, the fraud landscape has seen new threats emerge: outlined below are the top ten fraud trends that on the minds of credit unions and FIs for 2011.

1. Card-not-present fraud.

- Across the financial services industry, card-not-present (CNP) fraud is currently a top-of-mind concern not just among larger financial institutions, but also among credit union fraud shops.
- With more and more consumers becoming comfortable with online purchases, fraudsters' focus on perpetrating CNP fraud has been rising in tandem. While larger online merchants have standard fraud checks in place (e.g., address verification, card security verification, and credit card authentication), not all online merchants have such security measures implemented, leaving the onus of fraud prevention/detection on issuers.
- Credit unions must ensure standard fraud prevention/detection on their end, utilizing basic fraud tools (e.g., real-time decisioning, name/address match) provided by their card processor to assess transaction risk.

2. ATM, POS and self-service terminal skimming.

- Skimming hit an all-time high in 2010 and is expected to continue into this year. Recent attacks have ranged from traditional ATM skimming and incidents at merchant point-of-sale systems, to skimming devices installed at gas station pumps.
- More recent ATM "blitz" attacks, which involve simultaneous withdrawal of funds from multiple ATMs in different locations, reveal increasing sophistication and coordination among counterfeit card operations.
- Credit unions need to make sure their ATMs are secure and are encouraged to regularly check their ATMs, carefully checking for anything that may look abnormal or out of the ordinary. In addition, it is important that credit unions ensure that the video camera is in working order and has a good view of the machine, and that they educate members by emphasizing the importance of protecting PIN numbers.

3. Data breaches.

- More than 500 financial institutions were impacted by the Heartland breach, and a number of credit unions continue to be significantly affected by the aftermath of this large-scale data leak.
- Credit unions should consider exploring any data compromise solutions or services that may be offered by their card processor. Some solutions allow issuers to automate the handling and managing of compromised accounts for account blocking decisioning, card reissuance, cardholder notification and account monitoring.

Top Ten Trends Impacting Credit Unions in 2011

4. Social engineering schemes.

- Phishing schemes have continued to evolve in sophistication, utilizing multiple channels to engage potential victims. Text phishing and VoIP phishing (smishing and vishing, respectively) are newer forms of social engineering utilizing the mobile and VoIP channels.

5. "Fraud-as-a-service".

- Industry fraud experts have begun to see a trend in which criminal organizations are creating and selling fraud schemes as a "service," essentially commoditizing and managing fraud as a for-profit business.
- An example of this feat would be a basic Trojan kit that can be purchased online, with the provider actually having a support/member service number and providing push-outs of updated versions.
- Credit unions can stay on top such emerging trends by accessing educational resources provided through their card processor.

6. Internet information sharing, social networking and cyber-warfare.

- Financial institutions have been forced to confront the Internet's new realities, particularly the potential for reputational risk, data security concerns, and power of distributed network actions.
- The correlation between fraud and social networking is not to be taken lightly. Research has found that people using social networking for five or more years are twice as likely as those newer to social networking sites to suffer identity fraud (6.9% for five-plus-year users vs. 3.2% for newer users vs. 3.4% for non-users).[1]

7. Mobile malware.

- Software flaws within common mobile browser platforms provide the first credible opening for widespread mobile malware in the United States. McAfee, a security technology company, noted a 46 percent increase[2] in the amount of malware created for mobile devices from 2009 to 2010.
- Financial institution developers must see the mobile device as 1) a computer and 2) a computer platform distinct from desktop systems. They should follow secure software development lifecycle guidance and applications should run within their own mobile environment independent of browser and operating system vulnerabilities (a feature unique to the mobile platform.)

8. Fraud is down overall – but where are the fraudsters headed?

- Credit unions could expect increased attacks as fraudsters respond to tougher screening at larger institutions. If the big FIs are doing a better job of mitigating criminals, the fraud operations of credit unions and smaller financial institutions may well see more pressure.

[1] **2011 Identity Fraud Survey Report**, Javelin Strategy & Research, February 2011.
[2] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf

Top Ten Trends Impacting Credit Unions in 2011

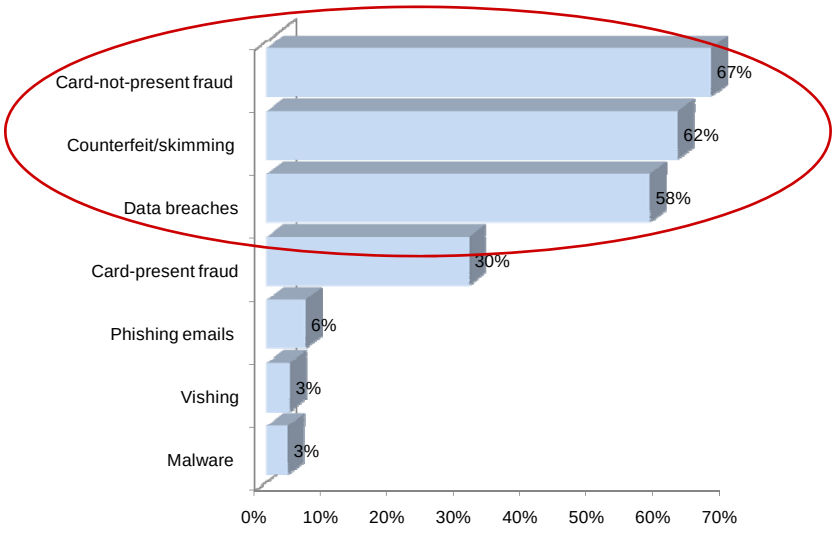
9. ATM malware.

- Although the biggest (and growing) problem consists of ATM fraud in the form of skimming, recent malware attacks in Eastern Europe and Latin America have raised new concerns about logical threats to ATMs.
- ATM malware aims to capture account numbers and PINs from the machine's transaction application and deliver it to the perpetrator on a receipt printed from the machine in an encrypted format, or to a data storage device hidden in the card reader. A thief could also command the machine to eject whatever cash was inside the machine. (A fully loaded bank ATM can hold up to $600,000.)
- A researcher at last year's Black Hat conference (the international technical information security conference held annually) demonstrated two hacks against ATMs, one of which was remote attack. Using a remote attack tool, the researcher was able to exploit the authentication-bypass vulnerability in the machine's remote monitoring feature, upload software, and overwrite the entire firmware on the system, allowing him to install malware on the machine.

10. First-party fraud.

- First-party fraud, also referred to as "friendly fraud" or "bust-out fraud," typically involves a member obtaining a credit card with no intention of repayment. In some cases, first-party fraud perpetrators may use synthetic identity information or mask their real identification.
- Specialized criminal gangs are now honing in on financial institutions with counterfeit identity information and sophisticated knowledge of lending procedures. Upon establishing a synthetic identity, the fraudster can build credit and obtain multiple financial products.

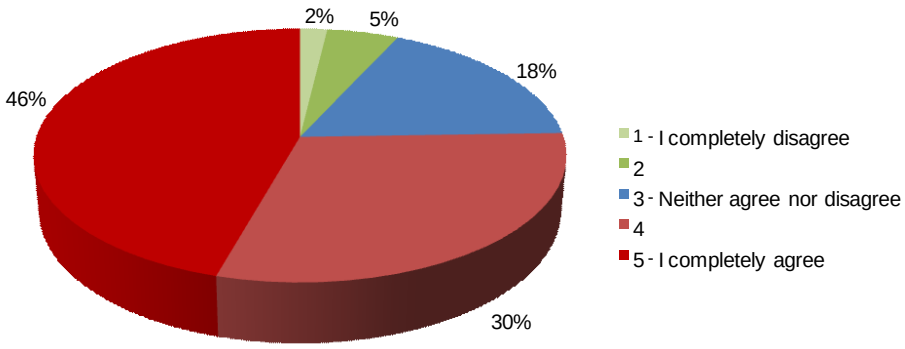
CSCU Survey Results Reveal Card-not-Present Fraud, Counterfeit/Skimming, and Data Breaches Represent the Greatest Fraud Challenges



CSCU Member Survey Results: What are Credit Unions' Current Opinions on Fraud?

More than Three in Four CSCU Members Believe Card Fraud is Increasing

Percentage of Who Believe "Card Fraud is Increasing Among Credit Unions"



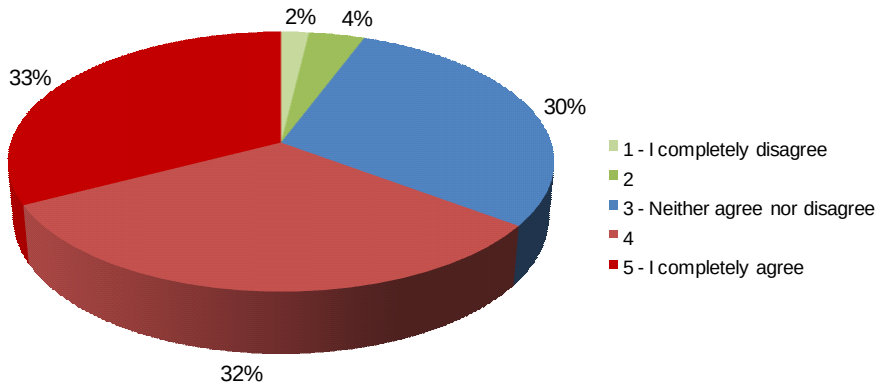
Please indicate, on a scale of 1 to 5, the extent to which you agree with the following statements. Let 1 represent "I completely disagree" and let 5 represent "I completely agree."

November 2010; N= 261
Base: CSCU members

261 CSCU members were surveyed in November 2010 to obtain credit union insights on fraud. Results revealed that the majority believe card fraud is on the rise among credit unions, with 76% agreeing with this statement. Most CSCU members also believe that fraudsters are heightening their attention on credit unions, with six in ten echoing this sentiment.

Six in Ten CSCU Members Believe Fraudsters are Increasing their Focus on Credit Unions

Percentage Who Believe "Fraudsters are increasingly targeting credit unions"

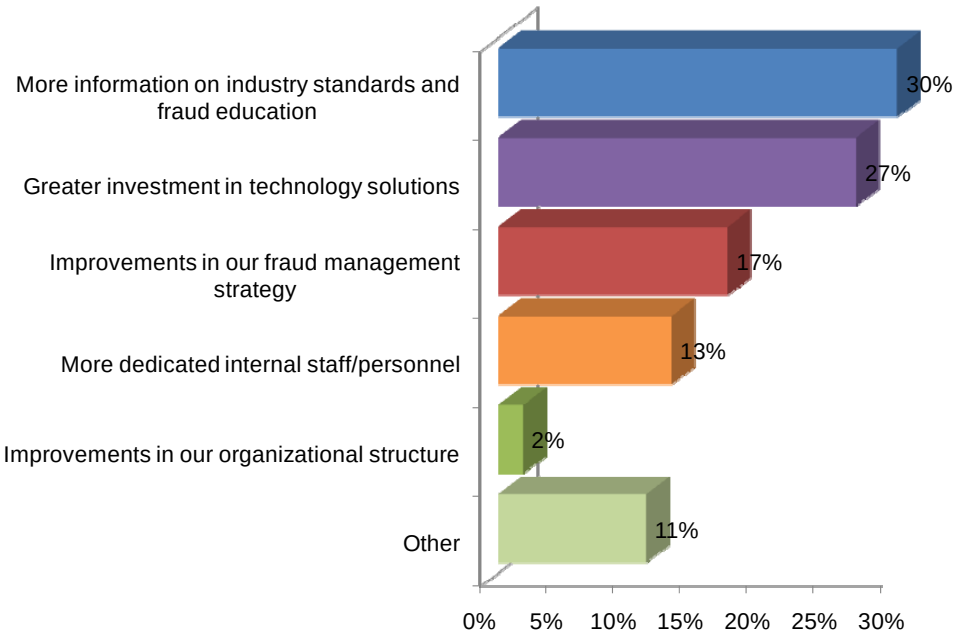


Please indicate, on a scale of 1 to 5, the extent to which you agree with the following statements. Let 1 represent "I completely disagree" and let 5 represent "I completely agree."

November 2010; N= 261
Base: CSCU members

CSCU Member Survey Results: What are Credit Unions' Current Opinions on Fraud?

CSCU Members Indicate Industry Standards and Fraud Education as their Greatest Need



Having implied a belief in increased card fraud and heightened criminal interest in targeting credit unions, CSCU members have thus indicated industry standards/education and further investment in fraud technology as their greatest needs areas. Members have clearly pinpointed the need to better understand fraud through benchmarking, best practices, industry standards for security, while investing in additional fraud solutions in order to mitigate risk and lower losses. These two identified needs are crucial to forming effective strategies and solutions for fraud prevention and detection.

Recommendations

1. Member education is crucial.

- Credit unions need to educate their members on basic precautions to take when providing information both offline and online. Financial institutions have made strides in educating members on phishing, but criminals continue to evolve fraud mechanisms to heightened levels of sophistication, requiring financial institutions to regularly inform and educate consumers on the latest threats.
- Provide straightforward, easy-to-understand and easy-to-implement tips for fraud prevention. For example, education on avoiding phishing emails might include "we will never ask you for your social security number or your account number", "never click on unknown links", etc.

2. Real-time is the way to go.

- Some credit unions may not utilize a real-time fraud prevention solution because they are afraid of impact on members. If your credit union has not already done so, consider investing in a real-time decisioning -- this will have a tremendous impact on your fraud losses.

3. Ensure effective communication with your members.

- This can be achieved by engaging in something as basic as establishing and maintaining a good web presence. Provide a web site that is user-friendly, easy to navigate, and provides up-to-date information.
- Retaining accurate, up-to-date member contact information can be extremely beneficial to the effectiveness of reaching members in a timely manner.

4. Capitalize on the partnership you have with your card processor and know what they have to offer from a fraud mitigation perspective.

- Invest time to utilize the fraud resources that are available to your credit union. Most processors offer training, webinars, downloadable research papers online, industry events, and regular fraud meetings. Take advantage of these resources, which will allow you to share/learn about best practices in effective fraud mitigation.

5. Monitor, monitor, monitor!

- On the most basic level, monitor daily authorization reports, excessive activity and foreign transaction reporting.
- Frequently review authorization processing parameters such as name mismatching, daily cardholder spending limits and velocity controls.