FAQ Resource

October 2022

Let's Talk Fraud: Fraud Prevention Tactics

During our "Let's Talk Fraud" webinar series, we discuss strategic approaches to protect your accountholders and keep them educated and informed. Learn more prevention tactics and best practices with answers to these commonly asked questions.

Table of Contents

Fraud Education for Accountholders

Q: Do you think it's a good idea to provide screenshots on social media that help demonstrate not only what a platform looks like but how to use it?

A: When using social media we're helping accountholders, but also educating the bad actor out there and potentially highlighting a weak link. Be careful how much you share. A good rule of thumb can be to highlight general information, but consider excluding specifics, such as specific rules and regulations that bad actors may not know.

Q: What are best practices for upholding strong accountholder relations, while at the same time putting our best foot forward to prevent fraud?

A: Establishing strong authentication measures for all accounts and transactions is the most effective way to mitigate fraudulent access to your accountholders' information and funds, which in turn, will strengthen trust. Taking extra precautions to validate individuals are who they say they are will continue to protect your reputation and relationships with accountholders.

Register for "Let's Talk Fraud" to learn about the latest fraud prevention tools, tips, and strategies to safeguard your financial institution: ***alliedsolutions.net/lets-talk-fraud***

Proactively communicate with accountholders about any fraud mitigation procedures you have in place that may impact them. Examples include:

- Alerts for account login pages that explain why you require numerous pieces of information to authenticate the individual prior to processing transactions, distributing funds, or allowing account access
- Proactive communications about fraud practices you have in place, such as your travel alert policies
- Notify accountholders immediately before or after you close their checking account or block their card due to fraud suspicions

Fraud Education for Board Members

Q: How can we work with our board to promote an enterprise risk management (ERM) strategy?

A: Consult with other risk teams across your organization to uncover how an ERM strategy could improve business. If you receive push-back on adopting an ERM strategy, consider requesting a trial period where teams, processes, and tools are consolidated. Document and report trial outcomes.

Enhancements often include:

- Consolidation of processes and tools to save money, streamlined resources, and improved efficiencies
- Sharing of expertise to uncover and prevent more risks
- Improved communication across teams and software tools to flag risk warning signs more often and earlier on to reduce total loss exposures

Holiday Fraud

Q: What are some of the common scams and best way to prevent losses for financial institutions during the holiday season?

A: Common scams during the holidays:

- ATM fraud attacks
- Payment card fraud, including being able to bypass chip and contactless options
- Bad actors ordering merchandise to empty house or vacant location
- Check fraud, with additional job opportunities over the holiday, more checks distributed by mail
- Phishing attempts with calls acting as financial institution or charitable organization
- "Free" holiday cash offers through from payment apps, like Zelle, Venmo, PayPal, Cash App

Best practices to combat holiday fraud:

- Educate your employees and accountholders to be on alert and to keep their financial information protected. Awareness is incredibly important over the holidays
- If they do receive a call/email/text, encourage them to reach out directly to the financial institution

Online Fraud

Q: What controls can we adopt to mitigate fraud risk when we don't have an online platform in place?

A: Employ a person or team who will look at all types of fraud coming in to help identify how it is taking place. If you cannot hire an expert, have current staff take on this role by researching common causes for the exposure and digging into the data to locate how and where the fraud happened to plug those holes. Centralizing all fraud management is a key risk measure to help detect, prevent, and mitigate the risk.

Loan Fraud

Q: What are the biggest fraud trends tied to loans?

A: The biggest loan fraud trends are:

- Loans taken out under a new account that were opened using a fake or stolen identity. Unsecured consumer loans being especially at risk, given they don't require as much information.
- Forged loan documents
- Counterfeited HELOC or line of credit loan payments deposited into an account and immediately withdrawn.

Q: How can we take measures to reduce the risk of a HELOC fraud attack?

A: HELOCs are at an especially high risk for fraud, given that these accounts are open-ended loans that offer criminals large financial gains. These attacks primarily occur one of the following ways:

- HELOC non-wire attacks: These come through shared branching or a branch location, asking for a disbursement not through the wire system, often in the form of a check or card
- HELOC wire attacks: These come through outgoing wires requested in a remote environment, often to international accounts. These pose a higher risk to the institution as the transactions are non-reversible once approved, and can often result in more than six figures in losses once the fraud is discovered.

Here are recommendations for managing these crimes:

- Educate accountholders and employees about how these crimes occur
- Encourage regular monitoring of accounts
- Place daily dollar and transaction limits for outgoing wires
- Confirm any transaction requests, including callbacks or texts to the accountholder, to approve a request
- Enforce authentication layers at every stage of the loan process
- Monitor HELOC accounts that suddenly have activity after a long period of inactivity
- Add more steps to confirm HELOC wire requests to international accounts
- Wait and confirm the identity of the requester before approving a new HELOC loan or releasing any HELOC funds

Internal Fraud

Q: Are there ways to detect or prevent money laundering in its infancy to stop these crimes?

A: Strong internal control systems can reduce the opportunity for money laundering. Consider adopting the following measures to more effectively prevent these and other internal fraud crimes:

- Mandatory dual controls
- Segregation of duties
- Audits, both surprise and planned
- Supervisory committee acting as a watch dog
- Whistleblower hotline for reporting fraud

Educate your employees about the warning signs for money laundering so they can help detect and report a possible attack early-on. Some examples of suspicious behavior include:

- An account is opened by a person not local to any of your branch locations
- An individual or business opening an account is reluctant to provide information outside of what they have already provided
- Another financial institution shares suspicions and/or negative information about an individual or business opening a new account
- Unusual transaction activity suddenly occurs on an account, such as a noticeable increase in the volume of transfers, cash transactions, or deposits in a single month
- Multiple accounts are opened by a single individual or business on or around the same time
- A loan is opened and immediately repaid

Authentication Fraud & ID Theft

Q: What are the warning signs for synthetic identity fraud?

A: Synthetic identity fraud blends fake and stolen information to create an entirely made-up identity. With data breaches being more and more of a reality, this type of fraud remains a huge risk especially with new account and new loan fraud.

Warning signs of a synthetic identity include:

- Credit report oddities, such as: payment defaults on previous loans, credit history or a long pause in credit history, or multiple retail card openings
- FICO score anomalies, such as: suspicious patterns in card, loan, or account openings, authorizations, or associated trades across lines of business

Q: What are the best techniques to manage stolen or synthetic identity fraud?

A: When it comes to preventing ID fraud your accountholders are your best source of protection. Here are some strategies for accountholders to detect and prevent these attacks:

- Use complex user names AND secure passwords for all online accounts
- Set up accounts to require more than just the user name and password (i.e., security question or text/email verification)
- Protect all devices with passwords, screen locks, face/thumbprint recognition, or other security settings
- Turn on biometric requirements on your phone and apps (i.e., fingerprint or face recognition)
- Sign-up for any account alerts
- Consider implementing a temporary credit freeze, to prevent unauthorized account or loan openings
- Track financial account activity closely and stay informed on common scams taking place
- Report suspicious or unauthorized activity immediately

Q: What is "bust-out fraud" and how can it be mitigated?

A: This type of scheme is where a fraudster applies for credit (i.e. credit cards, retail cards, home equity) under their name or using a synthetic identity. The individual builds a good credit history to increase the line of credit. The fraudster then maxes out all available lines of credit with the intention of not repaying and drops the account. These charges then go into collections and turn into charge-offs for organizations. These attacks happen on HELOCs and credit cards quite often, because they are open-ended loans that can receive continual credit increases.

Q: What are some tactics to prevent elder fraud?

A: Elder fraud prevention does not differ too much from other identity theft and scam prevention tips. The main difference is that the elder community is sometimes less likely to recognize the warning signs.

Warning signs include:

- Any unsolicited calls, texts, or emails asking for personal or financial information
- Messages with lots of typos
- Unsolicited emails with links or attachments
- Emails from an unknown sender - sometimes masked as a person you know, from an email address you don't recognize
- Requests from individuals or businesses using emotional messages or scare tactics to receive money

Best Practices to Prevent Fraud

Proactive mitigation strategies include:

- Monitor likely points of entry for fraud
- Set appropriate dollar limits and hold periods for ACH transfers, wires, and checks, as these are commonly used for online scams
- Invest in comprehensive liability coverage to protect against loss exposures
- Offer identity theft coverage with deeper fraud monitoring services (like dark web monitoring)
- Enlist the support of risk experts to audit and measure the strength of your policies and procedures
- Consider a representative to talk to your senior accountholders about elder abuse and fraud
- Engage the Elder Abuse Protective Services to share information with your senior accountholders and report any elder abuse to protective services.

Education to share with accountholders:

- Encourage accountholders to follow the FTC's posts or sign-up for their email alerts: consumer.ftc.gov/features/scam-alerts
- Inform elders you'd NEVER call, email, or text a request for personal or financial information
- Make fraud education and alerts readily available

Subscribe to receive more risk education: alliedsolutions.net/enews

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®