Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

Beware of Holiday Scams

SUMMARY

During the holiday season, the bad actors will engage in a variety of fraudulent activities to help put cash in their pockets. The holiday season is a time to give and receive, but it is not the time to allow the bad actors to receive. Confirming that you have fraud tools/solutions in place to help prevent or combat these holiday fraud threats is recommended. Here are some additional key prevention measures to minimize fraud around the holidays:

FRAUD THREATS AND MITIGATION STRATEGIES

Phishing and Social Engineering
Phishing will be at an all-time high over the holidays. When the cardholder attempts to make a purchase on the phishing website, the bad actor will steal the payment details and use the payment details at another website. Anti-phishing and social engineering measures include:

- Educate your cardholders to be on alert for phishing attempts while shopping online this holiday season and take extra caution when using their payment account data or personal information when visiting a merchant's website. If the offer is too good to be true, it could be a fake merchant on a phishing website.
- Educate your cardholders to be aware of being tricked into accessing phishing websites. Cardholders should take extra caution with popular large retailers, electronic merchants, airlines, travel booking, hotel and hospitality sites, and luxury goods retailers.
- Leverage multiple layers of authentication and educate your accountholders to NEVER respond to a phone call, email, or SMS text message or any other type of request. The bad actors may act as your financial institution and contact your cardholder to give them the OTP (one-time passcode) and other sensitive information to bypass the authentication layer.

Card Present
Bad actors install skimming devices to capture magnetic strip data at:

- POS devices at the merchant – If you allow fallback authorizations, you will likely see increased fraud.
- ATM/ITMs – If a deep insert skimmer is installed by the bad actor, you will not be able to detect it when inspecting your ATM/ITMs. Confirming with your ATM/ITM vendor that you have 100% anti-skimming technology in place on the physical ATM/ITMs is very important. In addition, blocking fallback authorizations at your ATM/ITMs will decline a counterfeit card if used.

Card Not Present
Digital skimming occurs when malicious code onto an online merchant website targets the checkout page, stealing account data from the checkout pages of the online merchants.

- Confirm you are using all available security tools to help identify and prevent this type of fraud, including:
    - 3D Secure for online purchases. If you are participating with 3D Secure, confirm you are using multiple authentication layers prior to the authorization. If you are not participating in 3D Secure and the online merchant is, the online merchant will charge all fraud back to you as the card issuer.
- Confirm you are watching the PINless authorizations.
    - Confirm you have daily dollar limits and daily number of transactions in place to prevent a run on PINless fraud.
    - If the online merchant is sending the authorization to your unaffiliated network, confirm with your network the layers of PINless security tools being checked prior to the authorization.

Jackpotting at the ATM/ITMs
This occurs when malware is installed and the bad actors attempt to remove your settings to make your settings unlimited and clean out the ATM/ITMs.

- Confirm you have all your settings in a controlled environment where, if an attempt is made to change the settings, the ATM/ITM will shut down and prevent a cash out.

New Membership Account Opening
The bad actors will attempt to join your financial institution and steal someone else's identity or create synthetic identities to conjure a person who does not exist. Take extra steps when opening new accounts in branch or online by:

- Using multiple layers to validate and confirm the ID of the new account opening.
- Lowering funding limits for new accounts and place a hold or extend a hold on the funds.
- Limit the types of products and services the new accountholder can obtain and consider a waiting period.
- Over the holidays you may see an increase in individuals attempting to join your financial institution so keep all team members on alert for anything unusual when an account is opened and limit the funding.

Paper Check Fraud
Paper check fraud is likely to increase over the holidays. Using the security tools available in the industry to help prevent or mitigate this type of fraud is paramount. Other fraud prevention measures include:

- On Us Checks – For corporate checks, cashier/teller checks, business member checks, HELOC checks consider using "payee positive pay" to prevent checks with altered or changes of any original check information from clearing. Your clearing/settlement (in house or vendor) would obtain a list of the checks each day and only clear the check items that were presented after verifying the payee, check number, and check amount.
- You may want to offer "payee positive pay" to your consumer checking accounts. Since most consumers write very few checks, this may be something a consumer would want you to offer to help prevent fraud on their account.
- US Treasury checks fraud persists. Continue to work with the US Treasury to address the check being deposited, then hold the funds, not offering immediate

availability. High dollar US Treasure checks need extra validation prior to any of the funds leaving the financial institution.
- US Treasury check reclamation period is one year and an additional 180 days at the close of the one-year period.

Outgoing Wire Request
During the holidays you will likely see an increase in outgoing wire requests. Authenticate and confirm the wire prior to the wire being sent. Once the wire is sent, it is gone.

- Perform multiple callbacks to your member at multiple phone numbers.
- Utilize a wire transfer agreement that contains specific wire transfer information and authentication procedures prior to processing the request.
- For internal employees, take extra precaution when an email is received requesting a wire transfer by having a face-to-face conversation with the employee that emailed the request before sending out the wire. This additional step could help mitigate business email scams.

Online Banking Credential Attacks
During the holidays, consumers will continue to be attacked by the bad actors to give up their personal and financial information. In addition, the bad actors continue to search to see what they can find on your financial institution and your accountholders.

- Key attacks are the username and password. We strongly encourage the use of multi factor authentication with all other security tools to help restrict the bad actor from getting into an online banking account or being able to use P2P, bill pay or any other payment methods to send money out the door to the bad actor or their mule.
- Educate the consumer to stay alert to anything that seems suspicious and to let you know as soon as possible.
- Set lower limits to help reduce the outgoing of funds. Many financial institutions increase the outgoing daily limits during the holidays and the bad actors know this.

Education is Key
Educational awareness for your employees and consumers of what the bad actors are up to this holiday season is critical. Continue to educate your cardholders to be on high alert during the holidays when using their physical card or card number (shopping online) and to report any unusual activity.

- Advise cardholders to monitor their card account daily transaction activity.
- Confirm your cardholders have signed up for text alerts to receive a notification every time their card is used.

RISK MITIGATION RESOURCES

- Refer to Visa's recent security alert.
- Learn more about transactional fraud solutions here.
- Find out how to reengage your inactive accountholders with these solutions.
- Simplify and reduce your payment for processing and production while increasing usage and revenue with this solution.
- Find out why paper check fraud is rampant.
- Visit the "Seasonal Scams" section of our fraud library for more resources.

LinkedIn Facebook