Manage **Risk**

Holiday Scam Prevention Checklists For Financial Institutions and Consumers

FRAUD MITIGATION CHECKLIST

Created By: Ann Davidson, Vice President of Risk Consulting

Allied Solutions, LLC

Last Updated: August 2017

Below are two checklists that address the heightened fraud activity that occurs during the holidays: the first checklist contains precautionary measures for your financial institution to follow to detect and prevent fraudulent activity during the holidays (and year round); the second checklist contains precautionary measures to share with your consumers to help them protect themselves from these holiday attacks:

FINANCIAL INSTITUTION HOLIDAY SCAM PREVENTION CHECKLIST:

- ✓ Educate cardholders about the heightened risk of attacks and scams during the holiday season, such as phishing attacks, scams where the member is asked to pay the scammer money, and recruitment scams where the member is asked to pay a bit of money up front to earn more money later on.
    - If you are aware of a scam, place the scam on your website, in your newsletter, and/or in the lobby of your branches to inform consumers.
    - Share information about scams with your employees.
    - Consider setting up a hot line for consumers to call if they are suspicious of any fraud activity.
- ✓ Watch for an uptick in online payment card fraud.
- ✓ Validate if the fraud is "card present" versus "card-not-present" to find out where the fraud is happening.
- ✓ Ensure you have comprehensive layers of security and authentication for both card-present and card-not-present transactions.
- ✓ Immediately report if you are seeing an increase in fraud to the card associations; also report the common point of compromise if one is identified.
- ✓ Strongly consider immediately blocking and reissuing potentially compromised cards to prevent future risk.
- ✓ Recommend to staff and members that they more closely and more frequently monitor ACH items, outgoing wires, and online transaction activity on all of their cards and accounts to look out for any unauthorized activity. Inform them to pay special attention to ACH items and outgoing wires.
- ✓ Utilize promotional and communications tools to increase the proliferation of information to your credit union staff and members about the increased likelihood of scams and attacks during the holiday season.
- ✓ Flag or block any unusual out-of-state card purchases. Inform members to alert you if they are traveling over the holidays, so that they are not affected by these preventative measures.
- ✓ Monitor any type of card fraud to help identify a card breach. Look for a common point of compromise and report it to the fraud department at the card association (i.e. Visa or MasterCard) immediately.
- ✓ Ensure that your credit union is receiving Visa alerts (CAMs) or MasterCard alerts regarding compromised cards and/or regarding information about the type of card data at risk (i.e. Track 1, Track 2, etc.).
- ✓ Determine if you will block and reissue or monitor compromised card numbers. In cases where the full unaltered magnetic stripe has been compromised, it is strongly recommended to block and reissue the card data.
- ✓ Contact cardholders to let them know when they are part of the compromised breach.
- ✓ Share a message on your website or phone system with any updates about the breach.
- ✓ Monitor PIN change activity. The criminal may make multiple attempts to perform a PIN change in order to obtain card data.
- ✓ Review daily dollar limits for signature, internet, and PIN transactions and offer members the option to lower their daily card limits over the holiday season.

- ✓ Watch for multiple payments on the same day or within days of each other on credit card accounts and do not provide availability of a payment to the credit card holder until other payments clear.
- ✓ Watch for increased cash disbursements (advances) being performed on non-credit union issued cards at the teller counter.
- ✓ Utilize an anti-skimming device on your ATMs to help prevent skimming.
- ✓ Utilize multiple layers of authentication when validating and sending out ACH and wire transactions both online and in-person to help prevent any unauthorized withdrawals of members' funds.
- ✓ Perform a review of your fraud risk tools and programs to assess their effectiveness.
- ✓ Continue to enhance your fraud protection strategies and your fraud management systems to help prevent card exposure.

CONSUMER HOLIDAY SCAM PREVENTION CHECKLIST:

- ✓ Place a security credit freeze on credit reports with all of the credit bureaus.
- ✓ Sign up for free fraud alerts from credit bureaus.
- ✓ Secure home computers, tablets, and mobile devices with a firewall and antivirus software before performing an online transaction.
- ✓ Avoid free downloadable applications for mobile devices since they may be infected with viruses and/or malware.
- ✓ Take extra time to monitor accounts closely for any type of unauthorized activity.
- ✓ When shopping online, remember to exit the site.
- ✓ Only use a private network when shopping or performing account activity online.
- ✓ Check out sellers before purchasing items.
- ✓ Cover hand when entering PIN at a store or on an ATM.
- ✓ Use the chip technology for all chip enabled cards.
- ✓ Watch merchants perform purchase sales to be on the lookout for any suspicious activity.
- ✓ Review card account transactions daily to uncover any unauthorized activity.
- ✓ Always save purchase receipts.
- ✓ Inform financial institution(s) of any travel activity.
- ✓ Consider requesting lower daily dollar limits on account transactions.
- ✓ Subscribe to fraud alerts.
- ✓ Be extremely cautious when making any online purchases.
- ✓ Keep private account/PIN/card information in a secure location.
- ✓ If contacted about card fraud, contact financial institution directly to confirm the fraud call's validity – DON'T EVER provide financial information to callers.

Allied's risk specialists are available to help your financial institution detect and thwart fraud attempts in their infancy. Contact us immediately to find out more.