RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: **Awareness** | Watch | Warning

Fraudsters Don't Take Time Off During the Holiday Season

This time of year, consumers are inundated with Black Friday and Cyber Monday promotions and enticing deals. While the holiday selling season means a spike in online and in-store traffic and sales, it also brings more fraud. Unfortunately, fraudsters don't take time off during the holiday season. Common fraud types include account takeovers, discount and coupon abuse, return abuse, payments fraud, and scams. Educate your members, so they don't fall victim to fraud during what should be a cheerful season.

Details

Fraud attacks increased by 13% last year during the holidays, according to the 2018 Fraud Attack Index from Forter. With holiday shopping just around the corner, increased online and in-store fraud is anticipated.

Unfortunately, many of these risks are outside of credit union control. Your members are vulnerable to common card fraud and other holiday scams at this time of the year.

- When shopping online don't be fooled by a fake, look-alike, or spoofed website, as it may contain malware to capture sensitive member information.
- With significant online orders, fraudsters can use shipping confirmation messages as their hook – again, beware; it may contain a link with malware.
- Scammers recognize the holidays as a popular giving season, so watch for fake emails, social media sites, or text messages promoting phony charities looking for donations.
- Be sure to apply in-person or go to a business' website to validate holiday jobs at delivery services and retailers. While it seems like they're looking for extra help, it could be another way to capture personal information.
- Beware of people asking for payment in the form of prepaid cards, gift cards, wire transfers, or going through a third party. These types of payments are typically not traceable.
- Remain aware of where you are at. Be on the lookout for ATM tampering or anything suspicious. Always survey your surroundings for safety.

Date: November 16, 2018

Risk Category: Consumer Payments, Card Fraud, Scams, Cybersecurity

States: All

Share with:

- ☐ Executive Management
- ☐ Front-Line Staff / Tellers
- ☐ Marketing
- ☐ Member Services / New Accounts
- ☐ Plastic Cards Department
- ☐ Risk Manager

To share risk insights or gain additional assistance:

- Report a RISK Alert
- Ask a Risk Consultant
- Contact a CUNA Mutual Group Risk & Compliance Consultant
  - **800.637.2676**
  - riskconsultant@cunamutual.com

Fraudsters Don't Take Time Off During the Holiday Season

Risk Mitigation

Educate your staff and members with these tips:

Member Tips:

- Sign up for transaction alerts to monitor for unauthorized transactions.
- Pay attention to emails, links, and websites. Think before you click!
- Ensure home computers, laptops and mobile devices are protected with antivirus, anti-spyware, and a firewall.
- Close shopping websites or turn off computer, tablet, or mobile device.
- Be cautious when using ATMs or gas pumps for skimming or shimming devices. For gas pumps, try to use the pump closest to the entrance door as they are less likely to be a target for skimmers.
- Encourage your members to review their accounts daily and report any discrepancies immediately.

Credit Union Tips:

- Check your card parameter settings and current fraud rules to ensure they are in alignment with expectations. Use the holiday season as a trigger to conduct a check-up at least quarterly or more frequently as your card fraud evolves.
- Reevaluate your fallback transaction rules and consider blocking all fallback transactions at ATMs as these are more susceptible to fraud.
- Watch for friendly fraud perpetrated by members. Train staff with a script addressing common objections. This can help with a more positive experience while deterring friendly fraud. Consider not reissuing cards to "repeat" offenders
- Monitor card reports daily for common patterns and fraud.
- Inspect ATMs daily if possible to ensure your machines are not targeted.
- Consider implementing technology such as knowledge-based authentication and multifactor authentication to detect synthetic identity fraud and to authenticate your members.
- Consider promoting mobile payment methods if you offer them.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

Review these specific resources for more information:

- Protect Yourself – Member Protection Tips
- Friendly Fraud & Error Resolution Overview
- Fallback Transactions / EMV Overview
- The Rise of Social Engineering Fraud
- An Employee's Guide to Phishing Emails
- ATM Inspection Checklist

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for white papers & checklists
- Webinars and Education
- RISK Alerts Library

Check out these areas of practice to help you manage pressing risks.

The Protection Resource Center requires a User ID and Password.

Interested in learning more about fraud, holiday scams, and other emerging risks?
Contact CUNA Mutual Group's Risk & Compliance Solutions at **800.637.2676** or by email at riskconsultant@cunamutual.com for additional risk insights.