Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

Account Takeover Fraud Critical Update

Financial Crimes Enforcement Network (FinCEN) issues notice on the use of counterfeit U.S. passport cards to perpetrate identity theft and fraud schemes at financial institutions.

SUMMARY

On April 15, the U.S. Department of the Treasury's FinCEN, in close coordination with the Department of State's Diplomatic Security Service, issued a notice to financial institutions on fraud schemes related to the use of counterfeit U.S. passport cards. The notice provides an overview of typologies associated with U.S. passport card fraud, highlights select red flags to assist financial institutions in identifying and reporting suspicious activity, and reminds financial institutions of their reporting requirements under the Bank Secrecy Act.

- Read further details in the FinCEN news release
- Review the FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions

---

Account Takeover Fraud Risk Alert originally sent on February 7, 2024

THE FRAUD FALLOUT

Account takeover attacks are one of the hardest threats for a financial institution to detect because often the user and device are trusted and genuine. Despite accountholder education, people continue to fall victim to these scams and credit unions continue to report large losses and reputational harm from this fraudulent activity.

HOW THE FRAUD IS EXECUTED

To take over an account, fraudsters are phishing, spoofing, and using social engineering against your accountholders via phone calls, text messages, emails, or chat and **pretending to be your financial institution's fraud team**

1. **The request:** The fraudster requests that your accountholder provide them with multiple authentication information such as online banking username and password, PIN, security codes, 6-digit code, and/or account number in attempt to drain the accountholder of their funds. They may also ask the accountholder to verify information such as card number, PIN and CVV/CVC, providing everything they need

to counterfeit a card. Accountholders continue to be fooled into thinking it is your institution's fraud team wanting to help them.
2. **The transfer:** The accountholder can be manipulated by the fraudster into performing the transaction and sending the funds to the fraudster.
3. **The takeover:** The fraudster may also contact your financial institution or your third-party vendors call center to place a travel alert for debit or credit card transactions so the fraud can be permitted in other states or countries.

MITIGATION STEPS

To avoid losses, take into consideration the following controls:

- Always include a statement in texts and emails when sending a passcode. For example: "If you did not request this passcode, contact your financial institution immediately. Don't share this passcode with anyone. Financial institution employees will never ask for this passcode."
- Warn accountholders of text message (smishing) and phone call (vishing) scams. Educate accountholders not to respond to any text messages or phone calls, even if they appear to come from their banking institution. Advise them to call using a reliable phone number to question any text messages, chats, or phone calls supposedly from their banking institution.
- Use a behavioral biometric solution that continuously searches a user's physical and cognitive digital behavior to distinguish between genuine users and cybercriminals.
- Require that accountholders register their devices, use device recognition, and geo location.
- Consider alternatives for phone, email, or address changes rather than allowing these changes within your online banking platform.
- Implement lower daily limits for new users for the first few payment app (ACH) transactions to reduce risk exposure.
- Block or delay transfers following a password change.
- Encourage accountholders to sign up for text alerts for credit/debit card transactions.
- Encourage accountholders to sign up for free freeze with the credit reporting agencies, limiting unauthorized use.

RISK MITIGATION RESOURCES

- Check out Allied's Risk Resource Library

The information presented in this document is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this document.