Allied Solutions

Allied INSIGHTS
Fraud & Security
RISK ALERTS

Timely insights to protect against fraud and mitigate risks

HELOC Fraud

SUMMARY

The industry has seen an uptick in fraudulent withdrawals on accounts that have Home Equity Lines of Credit (HELOCs). HELOC fraud losses can be especially large due to the high credit limits, ease of access to the funds, and generally no additional layers of transaction monitoring for these funds. Fraudsters exploit weaknesses in authentication and compromised consumer personally identifiable information (PII) to gain unauthorized access to HELOC funds, depleting them before the genuine accountholder has time to recognize the suspicious activity. We have heard from financial institutions that have experienced losses both at their own financial institutions and through shared branch withdrawal.

WHY ARE HELOCS TARGETED?

HELOCs may be desirable for bad actors for several reasons.

High Available Credit Limits: Many financial institutions issue HELOCs at the highest possible loan-to-value ratio; this is intended to give the accountholder the most leverage and flexibility to use equity in their homes for any number of reasons.

Easy Access to Credit Lines: While the intention is to provide the accountholder with unfettered access to their funds, this access also proves beneficial to the bad actors. Many financial institutions allow accountholders to access their lines of credit in branches, through shared branch facilities, in online banking, or even at ATMs/ITMs. The ability to clear checks directly from the line of credit account is now less common.

Relatively Easy to Locate Accounts: Because HELOCs are generally secured by the accountholder's property, a lien is filed with the public records agency in that jurisdiction. Unfortunately, public records are accessible to anyone who wishes to look for the information.

Compromised Consumer Data: Over the past several years, there have been countless data breaches — in fact, seven of the 10 largest data breaches have occurred in the past five years, resulting in billions of records being compromised. Because this compromised data is in circulation, it might be possible for a bad actor to have all the information they need to access your accountholder's funds

without needing to phish them for information.

RISK MITIGATION STEPS

Employee Training/Education: Make sure that your branch staff and call center employees are alert to potential fraudsters. Call center employees might be used by fraudsters to obtain information on the accountholder or to conduct transfers. Accounts with suspicious calls should be noted and/or restricted until verified with the legitimate accountholder. Branch staff should look for transactions involving HELOCs or withdrawals after a transfer is made from a HELOC. We have seen some instances where the ID being presented is not the same as the one saved in the financial institution's records.

Consider Restricting Access to HELOC Funds: For shared branch transactions, consider setting the risk tolerance level to low (since fraud rules are tailored to tolerance level), not allowing HELOC advances and limiting withdrawal amounts. Consider opt-out policies for shared branching. If you allow accountholders to make advances through online banking systems, consider requiring step-up authentication or other layers of security to verify the transfers.

Monitoring: Verify that HELOCs and other similar revolving credit products are included in your fraud monitoring system or reports. Depending on the volume of advances at your financial institution, consider reviewing all transactions for potential fraud.

Educate Your Accountholders: Be sure to inform any accountholder with a HELOC to closely monitor their accounts, looking for any unusual or unrecognized activity. Encourage accountholders to enroll in transaction alerts to be notified of activity before they receive their periodic statement.

RISK MITIGATION RESOURCES

- Watch Cooperative Credit Union Association’s Shared Branching Fraud Webinar
- Sign up for our Let’s Talk Fraud quarterly webinars
- View additional risk resources
- Visit our NEW Fraud Prevention Center!

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net