Home Equity Line of Credit (HELOC) scams continue to be a costly and challenging issue for financial institutions. Wire transfer fraud can easily reach millions of dollars, and with advancements in technology, such as online databases for county clerk records, online banking and online title searching, data commonly used by financial institutions to verify customer identity for wire transactions is routinely and easily comprised.

TRAVELERS

Several financial institutions have fallen victim to losses arising out of wire transfer and check forgery schemes targeting HELOC accounts and have taken action to mitigate the risk of future loss experience. Institutions that place a high value on their customer service and customer confidence in the institution's security against wire transfer fraud have implemented risk mitigation upgrades to their operations to help solidify customer confidence. According to Travelers, the following steps are initiatives that can help to eliminate, or at least significantly reduce, losses arising out of HELOC fraud scams:

- Place greater emphasis on getting full account numbers from callers;
- Phrase verification questions so that the caller is providing the information, rather than simply confirming what the financial institution has on file;
- Remove items from the list of authentication options (such as mother's maiden name and date of birth) that have become "public information" through social media websites and venues;
- Train employees who field calls to verify authentication items in a specific order and not skip to other items if the caller cannot verify the requested information;
- Train personnel with an updated full fraud-awareness module to help employees identify warning signs of fraud;
- Encourage customers to set up PIN numbers if the automated phone system allows it;
- Update customer account files with driver's license numbers, if not copies of the entire driver's license (or other government-issued ID if there is no driver's license);
- Utilize a mandatory callback procedure for all customer-not-present wire transfer requests;
- Use a password to authenticate customers rather than commonly compromised information and only allow in-person modification of passwords and key account information;
- Consider requiring full balance transfers (or transfers up to a certain percentage of the available funds) to be made in person while placing a reasonable monetary limit (or percentage limit) on customer-not-present wire transfer requests;
- Establish a reporting procedure which refers all suspicious wire transfer requests to a higher level of authority for confirmation/processing;
- Require a dual telephone confirmation procedure where the financial institution calls the home phone of the customer as well as an alternate number, such as a mobile phone or work phone;
- Establish an automatic two-day holding pattern anytime a request is made to initiate a wire transfer from a HELOC account to a foreign bank account within which time the financial institution ensures accurate verification and deters fraudsters seeking immediate processing;
- Verify change of address or phone number requests with a call to the customer's phone number on file;

- Customize specific and unique verification questions and procedures with an account holder/customer that can only be modified in-person.

Technology has made it easier than ever for bad actors to obtain data that is commonly used by financial institutions to verify the identity of their customers. That's why financial institutions must utilize robust authentication procedures to protect their customers – and themselves – from wire transfer fraud. This includes greater awareness, updated and vigilant policies, procedures and training, and implementing imaginative and unique verification procedures to help reduce the risk of sustaining losses arising out of wire transfer fraud targeting HELOC accounts.

Travelers is committed to managing and mitigating risks and exposures, and does so backed by financial stability and a dedicated team – from underwriters to claim professionals – whose mission is to insure and protect a company's assets. For more information, visit www.travelers.com.