UNDERSTANDING *HELOC SCAMS*

DURING THE CORONAVIRUS OUTBREAK

Eight ways to avoid forgery schemes.

Financial institutions around the country continue to fall victim to losses arising out of wire transfer and forgery schemes targeting HELOC accounts. Consider these tips to avoid being the subject of such fraudulent activity.

1. Check the Information. Require full account numbers to remit a transfer. Fraudsters often attempt to use partial account numbers that are available in the public record. If there is a change of address or phone number requested, verify such information with a call to the number on file or meet with the customer.

2. Carefully Select Verification Questions. Use authentication options that are not available in the public record, such as mother's maiden name and date of birth. Fraudsters will scan social media and the dark web to be prepared with basic information.

3. Require the Customer to Verify Answers. Phrase verification questions so that the caller is providing the information, rather than simply confirming what the financial institution has on file.

4. Adopt Multi-Factor Authentication. Encourage customers to set up pin numbers, update licenses and utilize mandatory callback procedures for all customers not present for wire transfer requests.

5. Set Limits! Consider requiring transfers up to a certain percentage or dollar amount of available funds to be made in person. Your customer should not be in a position where they need thousands of dollars immediately and cannot get to the bank.

6. Check and Confirm! Most fraud occurs at the single level employee approval. Establish a reporting procedure that refers all suspicious wire transfer requests to a higher level of authority for confirmation/processing.

7. Be Suspicious of Foreign Transfers! Most fraudsters operate outside of the United States. 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.

8. If it Sounds Suspicious, Be Suspicious! If a transaction seems suspicious, it probably is. Investigate and authenticate information. Customers will ultimately appreciate your dedication to protecting their funds.

KBA Kentucky Bankers Association