



Prevention TIPS

Actions You Can Take to Prevent Fraud at Your Credit Union

Actions Your Call Center Can Take

- Ask for Drivers License or alternate form of ID
- Review all large dollar HELOC advances
- Transfer call to team lead if:
 - Member fails two security questions
 - High Risk wire transfer requests
 - Employee family account
- Report suspicious calls to fraud personnel at your credit union
- Be suspect of international wires
- Impose additional verification questions that only the account holder would know

Wire Procedures You Can Implement

- Voice verification using previously recorded calls
- Call member's alternate phone numbers
- Review suspicious incoming wires (some fraud involves wires stopping at an account in the US prior to sending international)

Beware of Suspicious Activity

- Calls asking about how to wire money out
- Several calls made within a short period of time on a members account.
- Requests to change information on file or asking about information on file.
- Long pauses while asking verification information
- Answer security questions with incorrect answers but confident tone
- Large Home Equity Line of Credit Advance
- International destinations for advances.
- When unsure of answers criminal may try misdirecting conversation

Preventative Tools Your Credit Union Can Use

- Manually compare previously recorded member calls with the wire request calls
- Ensure your wire staff understands risks, this fraud, and is 100% confident wires are legitimate before sending. Follow through and provide the support they need if they decide not to send a wire.
- Educate frontline on social engineering, and provide them the support they need.

Best Practices in Prevention

- Involve fraud staff in high risk procedures. Make them easily accessible and/or locate them close to or perhaps within the operations department that handles wires
- Don't rely 100% on any verification process. Instead use a risk based approach to reviewing fraud.
- Create a layered approach to fraud – create high risk reports and review daily
- Recognize and reward employees that catch fraud
- Always consider the “evolution” of the threat