

## HELOC Wire Fraud Alert

This important information is provided about how criminals execute HELOC/wire scams so that you can take action to protect your members.

### *First some definitions*

**Social Engineering:** a non-technical intrusion that relies on human interaction and often involves tricking people into breaking normal security procedures and divulging confidential information.

**Data Mining:** the search for and review of Public Records, Social Networks, Credit Reports, Mailed Account Statements for the purpose of identity fraud.

**Malware:** short for malicious software that is designed to infiltrate a computer system without the owner's informed consent. [Key Loggers, Banking Trojans, Worms and Viruses]

**Dumpster-diving:** sifting through trash to find items that may be useful in identity theft.

**Insider Job:** employees using their position and/or computer access to steal valuable financial and intellectual information.

**Spoofing:** a person or program successfully masquerades as another by falsifying data.

**Phishing:** attempts to acquire sensitive information such as usernames, passwords and account and credit card details by masquerading as a trustworthy entity.

### *Criminals use various methods to gather member information*

- Data Mining of Public Records - like mortgage & title documents
- Mail Box Raids
- Viruses and Malware on members' computer
- Information found in member's garbage - "dumpster-diving"
- Pulling credit reports
- Credit Union or other Financial Institution employee passes info to criminal – "inside job"
- Telephone and Internet spoofing/phishing.

### **WARNING!**

The criminals have substantial account holder information. Inclusive of last transactions, family member names, account numbers, social security numbers, real estate information and automobile make and model. In many cases credit reports have been pulled on account holders prior to the fraud.

You must assume that any public information and information you mail to your member is known to the criminal.

### *How They Pull it Off*

#### **Criminals gather information:**

- Public records to obtain HELOC information & signature samples
- Facebook & Mailed Account Statements

- Conduct multiple calls to call center to social engineer the staff for additional information and to establish him/herself as member
- Criminal poses as member and requests CU to change home phone number or places a service disruption complaint with the phone company and asks for calls to be forwarded to 'New' number

**Posing as member:**

- Criminal, posing as member requests transfer from HELOC to checking account via fax
- Signature on Faxed request matches signature on file
- CU calls member's home phone of record to verify the request, but reaches criminal via the number criminals correctly respond to verification questions due to data-mining efforts
- CU processes wire

**Criminals make off with cash:**

- Wires are sent to either domestic or international accounts
- Domestic wires are promptly forwarded on to international destinations
- Once the money arrives at its international destination, the criminals make cash withdrawals

***Some Common Denominators***

Member has significant funds or large HELOC accounts

Transfers range from \$50k up to \$1M with 90% of the available credit line not uncommon

Destinations include Japan, Hong Kong, Russia and Singapore

Many of the verification calls have long delays on the criminal's side as they attempt to answer questions

Fraud usually goes unrecognized until member notes activity and contacts the CU

***Prevention***

**Be very cautious with wires that include the following:**

Fax request

Recent HELOC advance

Recent contact information change

International Wire

Member with no history of International Wires

**Additional Steps to Verify:**

Require members to visit a branch for large wire requests and ask for picture ID

Verify all large dollar HELOC advances;

Be suspicious and verify large international wires

Report suspicious phone calls to Fraud personnel

Perform extra level of verification for wire requests on accounts that had recent contact information changes

Do not fax forms to numbers outside your member's home area code without verification

Manually compare previously recorded member calls with the wire request calls – does the caller sound like your member?

Educate frontline staff on social engineering and support them when they have a suspicious caller; Assure your wire staff understands the risks and only processes wires when 100% confident they are legitimate; and recognize and reward employees that prevent fraud.

Involve fraud appropriate staff in developing high-risk wire procedures; Co-locate fraud/risk personnel with the operations department that handles wires

Don't rely 100% on any single verification process

Use a risk based approach to conducting verifications

Create a layered security approach to processing wires

Produce high risk reports and review them daily

Keep CU staff in involved

### ***Signs of Suspicious Activity***

- Calls asking how to wire transfer money
- Several member calls in a short period of time
- Requests to change member information on file
- Long pauses or incorrect answers when responding to questions
- Caller tries to redirect conversation when unsure of answers
- Signatures on multiple documents match exactly

### ***Sample Fraud Scenario***

**Background:** XYZ FCU has been a trusted financial partner in the community for over 50 years. David Smith has been a member for 42 of those years and uses the credit union for all of his financial needs, including a Home Equity Line of Credit, HELOC.

**Sample:** One morning a credit union Member Service Representative (MSR), answers a call from someone identifying himself as David Smith. Mr. Smith seems a bit slow in answering the security questions and you can sometimes hear papers shuffling. Once authenticated the caller requests a change to his home telephone number on file. During the same call he requests an International Wire Request form be faxed to a number outside his home area code. According to his file Mr. Smith was born in 1933 but his voice sounds more like someone in his twenties

Despite being a little uneasy about the call, the MSR changed the contact number, faxed the paperwork and did not notify management or the Risk Officer. Three weeks later the credit union receives a fax Mr. Smith requesting a \$94,000 advance against his HELOC.

The request has the right signature and appears to be in good order so it is processed.

The next week the credit union receives a FAXED International Wire Request form for \$94,000 to an account in Hong Kong. XYZ FCU procedures permit Members to fax domestic and international wire requests, as long as the confirmation call can be made to the home phone number on file.

Existing procedures don't say anything about checking whether the Members' contact information has been changed, but they do require full authentication of the member and verification of wire details.

Per procedures XYZ FCU calls Mr. Smith at his new phone number to authenticate his identity and verify the wire. Mr. Smith sounds a little anxious and he struggles with authentication questions again. Mr. Smith still doesn't sound like a man in his 70s. Mr. Smith gives an incorrect answer to a security question, but quickly complains about a member service issue. At the end of the call Mr. Smith asks about domestic wires.

Satisfied, the credit union employee completes the verification and submits the wire for processing.

### ***Outcome***

Credit Union employees followed procedures and even though they felt a little uneasy at times, the caller was persuasive and obviously knew information about the account.

The international wire was sent out, and eventually a domestic wire was requested and completed as well.

A few days after the last wire was sent, David Smith visits a branch to find out why he hasn't gotten his most recent monthly statement. Mr. Smith doesn't recall having changed over to the electronic statement and he seems shocked when told about the HELOC advance and wires from his account. It's only at this point that XYZ FCU investigates and discovers fraud.

### ***Lessons to be Learned***

Accepting faxed HELOC and wire requests opens a Credit Union to significant risks.

Be willing to use critical thinking when serving a member such as does their request make sense? Member Services Staff need to be aware of Social Engineering and Misdirection techniques that criminals will use to try to fool them.

If member services staff is careful about security and willing to question suspicious requests, criminals will probably go elsewhere.

### ***Conclusion***

In our current environment, Credit Unions must learn to balance member service and convenience with security. We are not serving our membership by quickly processing a wire transaction if it turns out to be fraudulent. Will our members really have an issue with us doing everything we can to protect them?

### ***Next Steps***

Request a copy of this presentation and review with all employees involved in your Credit union's wire transfer process. Immediately review your wire transfer verification procedures to add more robust/tighter security controls; and update your authentication process to include questions on non public information that is not mailed to your member.