

# **HELOC/Wire Fraud Alert**

**WEBCONFERENCE**

**1/4/08**



CREDIT UNION INFORMATION SECURITY PROFESSIONALS ASSOCIATION

**[WWW.CUISPA.ORG](http://WWW.CUISPA.ORG)**

(512)845-3142

## **Presentation Contributed By:**

Jeff Johnson  
Baxter CU

## **WebConference Panelists:**

Kelly Dowell, Executive Director, CUISPA  
(512)845-3142

John Mulkerin, KeyPoint CU

Tom Kuang, Schools Financial FCU

John Nutt, Lockheed FCU

Luanna Harmon, FBI

# Fraud Description

- Criminals gathering information from public land and deed records; HELOC information and signature samples
- Multiple inbound calls being made to call center
- Socially engineering call center staff for additional information “establishing” that he is the member
- Many of the calls have long delays on the criminal’s side
- Criminal poses as member and places a ‘service disruption’ complaint with the members’ home phone service provider
- Phone company forwards calls made to home phone number on record to the criminal.
- Some cases have involved updating phone records with institution through the call center.

# Description Continued

- Criminal requests wire transfer
- CU calls member's home phone to verify the wire, but is forwarded to bad guy.
- Faxed in wire request signatures match signatures on file.
- Wires are sent to either domestic or international accounts. Domestic wires are promptly forwarded onto international destinations.
- Transfer attempts range from \$50k up to \$1m with 90% of the available credit line not uncommon.
- Destinations include Japan, Honduras, Russia, Greece, etc.

# Elements of the fraud

- Gathering of public data
- Social engineering of institution's staff for additional information
- Social engineering of phone company

## WARNING:

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

# Preventive Action (internal)

- Call Center Adjustments
  - 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
  - Be suspect of international wires
  - Impose additional verification questions that only the account holder would know.
- Wire Procedures
  - Voice verification using previously recorded calls
  - Call member's alternate phone #'s
  - Review suspicious incoming wires (some fraud involves dropping at an account in the US prior to sending international

# External Support

- FBI - Cases Filed
  - **Luana Harmon** – (916) 874-6590 – #288A-SC-42055 [luanna.j.harmon@infraguard.org](mailto:luanna.j.harmon@infraguard.org)
    - Working on multiple cases with Credit Unions, assigned analyst to compile data from national cases
  - Alicia Wojtkonski – (301) 591-8503
  - Scott Marino – (732) 302-2920
- AT&T & Verizon
  - Reluctant to release any information
  - Referring to their Security Departments
  - They are taking this seriously
  - Little action or response at this point
- CUISPA
  - Organizing communication for institutions to share details
- CUNA Mutual Group
  - Multiple claims currently on file. Public awareness

# Effects on Member Service

- Phone talk times have increased one minute on average due to increased security verifications
- Some legitimate members are failing increased security questions – train frontline on how to handle

# Suspicious Activity

- Calls asking about how to wire \$ 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.
- They try to trip up the phone rep by misdirecting conversation, when unsure of answers.

# Preventative or Forensic Tools

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

# Best Practices in Prevention

- Involve fraud staff in high risk procedures – locate them closely if not within the operations department that handles wires
- Don't rely 100% on any verification process – 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 (with \$!)
- Always consider the “evolution” of the threat

# HELOC/Wire Fraud Alert

## WEBCAST DETAILS

131 Attendees

91 Credit Unions

23 CU's reported an incident(s)

21 Banks

6 Banks reported an incident(s)



CREDIT UNION INFORMATION SECURITY PROFESSIONALS ASSOCIATION

**[WWW.CUISPA.ORG](http://WWW.CUISPA.ORG)**

(512)845-3142