Urgent Identity Theft Fraud Notification and Best Practices to Acquirers
October 18, 2016

A recent rise in identity theft and account take-over fraud has shed light on the need for added safeguards for shared branching acquirer locations throughout the network. The primary fraud MO is a perpetrator utilizing member data to obtain a very good identification document (Driver's License, Government ID, etc.) and then going to a shared branching location to withdrawal funds—either check or cash. In the majority of these cases, the loss could have been prevented if the teller followed best practices and thoroughly compared the ID to the Member Verify response.

It is extremely important for tellers to carefully compare the identification information to the data sent by the issuer as shown on the teller screen, and the physical presence of the member performing the transaction. Below are the CO-OP Shared Branching identification rules and suggested best practice steps for tellers to follow.

Tellers MUST follow identification procedures found in the CO-OP Shared Branching Rules:

In examining the valid form of ID, tellers/MSRs will verify:

- Complete address (If the address on the ID is different from the system address, the teller will verbally inquire as to the address on file.)
- Last 4-digits of the member's or joint owner's social security number

Acquirers may also verify the following information:

- Member's date of birth (if provided by the issuer credit union)
- Phone number of record on the account
- Is there a joint owner and if so, what is the name?
- What types of accounts does the member have?

Additional Best Practices to be followed:

- Verify ID number if passed by the host credit union
- Compare the names and ensure proper spelling
- Use the ID Checking Guide for all unfamiliar IDs
    - Photocopy the ID if possible for large transactions
- If the teller platform displays "Last Shared Branch Visited" (check the number of visits and address of the last location in comparison to current location). If in doubt the teller should obtain additional verification by calling the host credit unions if possible or bringing the matter to a manager's attention

Be Alert:

- Be extra cautious of members asking for large check withdrawal
    - Take extra time to review the points above
    - Check the member's account history to see if they made a recent large withdrawal
- Check for nervousness of the individual conducting the transaction or if they appear fidgety or watching over their shoulders
- Do not hesitate to question a member about the nature of the transaction
- Get a second approval from a supervisor or manager

Effective Monday October 24, 2016 CO-OP Shared Branching grievance procedures will take into account the verification and best practice efforts of the acquiring location. If the credit union does not follow the above best practices, there is risk that the acquiring location may be negligent, and may result in the acquirer being liable for any losses that may have been prevented.

We appreciate your diligence and cooperation in helping protect your fellow credit unions from preventable fraudulent activity. We also ask that you implement the above best practices as quickly as possible but no later than Monday October 24th.

Please contact CO-OP Shared Branching Network Services with any questions at networkservices@co-opfs.org or 866-812-2872, option 2.

Sincerely,

Salvador Mendoza
Director of Network Support and Fraud Management

-####-