Risk Alert Reminder– Member Account Protection for Wire Transfers

Wire Transfer fraud with domestic and foreign implications continues to be a major concern and recent reports to various governmental agencies* have indicated a new twist by criminals to wire funds out of a member's financial institution account using a compromised email account. This scheme has impacted all types of banking institutions. Instead of contacting a financial institution by phone or fax, these criminals are successfully compromising email accounts and or spoofing email addresses to send wire transfer requests to the institutions.

Email account hacking is on the rise as evidenced by a fraud recently experienced by many where a criminal who has accessed an account sends an email communication to an individual’s contacts claiming an emergency and the need for funds to be sent immediately to assist the individual. The current wire transfer fraud begins when a criminal hacks into a person's email account to look for personal information which is then used to submit wire transfer requests. Any such hacking allows the criminal to view the person’s contact list and "sent" emails. Once financial information is found, they may send an email to the person's financial institution requesting an account balance. When an affirmative response is received, another email may then be sent requesting funds be wired to another financial account which may be domestic or foreign. A financial institution should be wary of claims that the requestor is only able to communicate by email due to illness or a death in the family.

When communicating with the CU, the criminal may use a slightly different or spoofed email address to maintain the scam. Instead of Joe.Smith@aol.com, they may change the address to Joe.Smyth@aol.com or they may alter the domain from .com to .net. Reports have also indicated that criminals have successfully altered the member’s email account settings to block the member’s receipt of legitimate emails from their financial institution.

The following risk controls have been identified to assist in minimizing the risk of loss:

- Only accept large dollar wire transfers requests if the member comes on site; discontinue accepting substantial dollar requests by phone, fax and email;
- Develop monetary thresholds for wire transfer requests submitted by phone, fax or electronic mail and continue to perform callbacks to verify authenticity;
- Establish a formalized written funds/wire transfer agreement with the appropriate levels of information to be provided by members for future transfer requests;
- Encourage members to place a password or pass code on their account to verify the authenticity of wire transfer requests;
- If a wire request is made through a faxed request form, do not rely on the signature of the member as such can be easily forged - this holds true for a notary signature as well;
- After receiving a wire request form, carefully review the member’s account to determine if the request is reasonable and falls within the historical activity of the member’s account;
· Follow your established and enforced written Callback policies and procedures which should include the following:
  o Ensure that the member's phone number has not changed in the last 30 days. If the member’s phone number was changed within that time frame, further non-electronic contact should occur with the member to ensure authenticity of the transfer;
  o When performing a callback, always listen for audible clues such as a lengthy delay for the call to connect and/or other clicking sounds which may indicate that someone has call forwarded the member’s phone;
· Provide frequent training sessions to employees on loss control procedures utilized in processing wire transfer requests.

*FINRA, FBI, Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Internet Crime Complaint Center (IC3)*