Risk Checklist

Financial Institution

Wire Transfer and ACH Fraud Prevention

Scammers continue to find weaknesses in the validation and authentication processes so they can obtain secure information, in order to fraudulently transfer and/or wire money to themselves. To prevent fraud, your financial institution must create multiple layers of authentication in the wire transfer and ACH payment processes, while also implementing the following best practices.

Allied Solutions

May 2021

Wire Transfer Fraud Prevention

- ☐ Implement multiple layers of authentication with your account holders, such as:
  - Create a unique PIN or passcode for outgoing wire requests.
  - Confirm a security question between the financial institution and the account holder.
  - Consider contacting account holders on their cell phone, work, and/or landline as one of the layers of authentication for wire requests. Never rely on only one call back telephone number.
- ☐ Consider not offering outgoing wires when the account holder is not present, since most wire fraud instances are happening in non-face-to-face environments. Do not accept wire transfer requests over the phone, via fax (even if they are notarized), through email, or by snail mail.
- ☐ If you do offer non-face-to-face outgoing wires, consider limiting the dollar amount.
- ☐ Consider not offering international wire requests or label outgoing international wire requests as "high risk" and take extra measure before performing the wire request.

Visit our website for more risk education:
alliedsolutions.net/resources

- ☐ Before performing an outgoing wire, confirm your financial institution and the account holder have signed and completed a wire transfer agreement that includes information about all of the authentication measures you require for wire transfers.
- ☐ Ensure employees monitor wires closely to report anything that may seem out of the ordinary and advise them to report any suspicion directly to senior management.
- ☐ Provide your staff with educational materials about wire fraud and wire fraud prevention.
- ☐ Do not post your wire policies and procedures publicly, as doing so will allow the scammer to spot weak areas to penetrate.
- ☐ Set daily transaction limits for account holders.
- ☐ Pay special attention to wires from a Home Equity Line of Credit (HELOC) as account holders with a HELOC loan are especially vulnerable targets for outgoing wire fraud.
- ☐ Restrict the IP addresses associated with your financial institution.
- ☐ Review – or have a risk prevention specialist review - your wire policies and procedures to make note of and repair any areas of weakness.

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

ACH Payment Fraud Prevention

Below is a list of measures to help your financial institution mitigate the risk of ACH payment fraud:

- ☐ Discontinue the practice of allowing ACH payments on credit card accounts.
- ☐ If a third party processor is offering ACH payments using an online process, first review the agreement, process, and potential liability associated with this payment process.
- ☐ Utilize ACH parameters to review large ACH payments or multiple ACH payments within the same day or within a few days of each other.
- ☐ Work with your ACH association to help understand the credit risk associated with ACH payments.
- ☐ Monitor daily ACH returns on settlement accounts.
- ☐ Review the following report types to help identify risk:
  - Credit card kiting reports
  - Over credit card limit reports
  - Reports of excessive activity on credit card accounts
  - Cash (disbursement) advance reports (Credit card MCC codes 6011 and 6012)
  - ACH Return reports
  - ACH Large dollar reports
  - ACH Payment reports
- ☐ Review the NACHA Operation Guidelines in the Rules Book on third party service providers.
- ☐ Review NCUA guidance on third party service providers.

Contact us to receive more risk education and support: alliedsolutions.net/enews.

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

975-R6-5.21