Protecting your Institution and Customers from Fraudulent Activity

Fraud...the mention of the word can make even the most seasoned bank employee shudder and rightfully so! Fraud can have far reaching impact for your bank and customers including: monetary losses, reputational risk, and penalties assessed by regulatory agencies. There are several simple steps you can take to help protect your account and your customer's accounts from fraudulent activity.

1. ***Regular Monitoring*** - your Daily Transaction Confirmations, ACH Acknowledgement Reports, DDA Statement and other regularly provided reports are critical steps you can take to monitor for fraud. (*For example, if you don't write checks on your UBB account, but suddenly are seeing items on your Daily Transaction confirmations or statements with a description of "Check" this likely indicates fraudulent activity).*
2. ***Limiting and protecting account information provided to your customers*** - When providing wiring instructions to your customers, do not provide your UBB DDA Account number. UBB's Incoming Wire Instructions instruct you to use your bank's routing number in the Beneficiary Bank FI field. This protects unauthorized individuals from gaining access to your DDA account number. (***If you are using an older version of the form that still asks for DDA, please access the newest version of the form in UNET, under Resources and then Wire Reference Info)***.
3. ***Don't be afraid to ask your customers questions!*** (For example, purpose of payment is most often a required International wire field. *If your customer isn't sure of the purpose or shares a purpose of payment that raises red flags, work with them to get additional information and encourage them to ask more questions).* **The same guidelines apply to foreign checks, most often purpose of the check is required.**
4. ***Follow your policies and procedures*** – When customers request to send an outgoing wire, gather information and follow the appropriate steps in call back, verification and validation of data.
5. ***Emails from customers –*** be especially cautious and take the proper steps to verify it is legitimate. (*For example, remitters/originators should be reminded to use contact information that is on file when paying invoices or sending payments).*
6. ***Verbal communication*** – have the originator and beneficiary been in contact? How do they validate they are not being scammed?
7. ***OFAC scanning services*** - it is easy to become complacent in approving potential OFAC matches. We understand the stress of trying to get wires or ACH transactions entered in UNET in a fast and efficient manner. We would caution you to treat every OFAC hit as a true potential match. Do your due diligence in researching those potential matches, document and save your research. **Your customers are depending on you!**

Fraud is on the rise, whether it is ACH, check, wire, or email, so we need to be vigilant and monitor, monitor, monitor! As fraudsters get more and more savvy, it may seem fraud is inevitable, but by implementing some of these simple procedures, you can make it much more difficult for the perpetrators to be successful. ***Let's work together to help prevent fraud!***