Fraudulent Funds Transfer—What You Need to Know

Q&A with Tracey Santor, CPCU, AFSB, AIC, bond product manager, financial institutions, Travelers Bond & Specialty Insurance

Q: What do you see as one of the biggest risks facing Community Banks right now?
A: On-line criminals fraudulently instructing financial institutions to send money to their accounts is a big concern. The act of wiring money from a bank account or line of credit to pay bills is easy and convenient, so more people are doing it. In fact, the primary clearing house for large banking transactions, Clearing House Interbank Payments System, or "CHIPS" reports that it moves approximately $1.5 trillion per day on its wireless network. The majority of these transactions take place without a problem but criminals have focused on hacking this method of transferring money to line their own pockets. With this in mind, funds transfer fraud and computer fraud are threats that every organization must consider.

Q: What is are fraudulent funds transfers?
A: When someone poses as a customer to take control of an account or line of credit to engage in unauthorized transactions.

Q: Can you provide an example?
A: Your institution's website receives what appears to be legitimate input from a business customer linking its payment account to an outside account at another institution. The username and password are valid and your other security procedures have been satisfied. Through your website, your institution then receives instructions to transfer funds from the customer's account to that outside account. Your institution complies. One week later, you are contacted by law enforcement and told that your customer was the victim of a scheme perpetrated by cyber-criminals; and fielding calls from the customer questioning your safeguards.

Q: Where does this leave my bank?
A: Your institution's security has not been directly attacked, but your customer's security was somehow lacking the ability to prevent an intrusion. Now, you're facing potential legal, regulatory, and maybe even reputational issues.

Q: What practices can my bank institute to help fight security breaches?
A: For instances like the one mentioned above, customer and employee education are key. Educate customers and employees on procedures that enable consistent oversight of payments and accounts, and may reduce fraud risk. These include: SSC/Payment Factory setups, Dual Custody practices, and ACH Positive Pay. Also, consider verification procedures that are independent and spread through the different departments of the financial institution and encourage your customers to do the same. Financial institutions should have discussions with their customers about purchasing commercial crime coverage which would protect the

customer under the Fraudulent Funds Transfer insuring agreement. Finally, institute Multi-Factor / Multi-Channel Payment Authentication whereby the bank practices using:

- Callbacks: prior verification of payment instructions to a predetermined telephone number
- Passwords & SMS ID Codes
- Out of band verification
- Other industry-accepted verification procedures

Additionally, banks should speak with an independent agent, who can recommend the right insurance solutions to help protect against such risks.

Q: What about the cost to my organization?
A: Cost concerns are important, but the cost to your business should this happen can be further reaching and include long-term damage to your reputation. Some security procedures may have a cost associated with them but things like employee and customer education are practically free and can save financial institutions and/or their customers from being victims.

Q: Where can I learn more?
A: In addition to insurance coverage that can help offset the impact of computer fraud risks, Travelers offers numerous educational resources, such as insightful loss-control articles and tips. Learn more here.