ALTA Rapid Response Plan for Wire Fraud Incidents

https://www.alta.org/file.cfm?name=ALTA-Rapid-Response-Plan-for-Wire-Fraud-Incidents

Time is of the essence – every second and minute counts.
Organize your team and make a plan in advance.
Be ready to act simultaneously and accomplish all of these steps as quickly as possible.

Step 1: Alert company management and your internal wire fraud response team.

Contact your team according to a pre-arranged plan (group email; group text):

- Owner / Manager
- Accounting / Finance / Treasurer
- IT / IT Security
- Legal Counsel
- Underwriter(s)

Step 2: Report Fraudulent Wire Transfers to the Sending and Receiving Banks.

- Contact the sending bank's fraud department and request that a recall of the wire be sent to the receiving bank because of fraud. Provide the details for the wire. Also request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain.
- Also call the receiving bank's fraud department to notify them that you have requested a recall of the wire because of fraud. Provide the details for the wire and request that the account be frozen.
- If a client or consumer was a victim and your bank/accounts were not directly involved, your client or customer will need to contact the bank themselves but you may have helpful information to share, too. Coordinate quickly!

Step 3: Inform the parties to the transaction (buyer, seller, real estate agents, broker, attorneys, underwriter, notary, etc.) using known, trusted, phone numbers for verbal verification.

If you're unsure about what to say, here's a sample: "There appears to have been [attempted] wire fraud associated with this transaction. We recommend that you review your email security and update passwords and take any other appropriate security measures immediately. For the remainder of this transaction, all communication will occur using known, trusted, telephone numbers."

Step 4: File a complaint with the FBI's Internet Crime Complaint Center (IC3).

Need help to get started? Visit www.alta.org/ic3how to see a two-minute how-to video.
Ready to go? Visit www.alta.org/ic3 and provide the following information:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- For Business Email Compromise (BEC) events, copy email header(s). Learn How at https://mxtoolbox.com/Public/Content/EmailHeaders/
- Any other relevant information that is necessary to support the claimant

Step 5: Report Fraudulent Wire Transfers and Attempts to Law Enforcement in the jurisdiction where the crime has occurred.

- Local Police/Sheriff: https://www.policeone.com/law-enforcement-directory/
- FBI Field Office: https://www.fbi.gov/contact-us/field-offices
  Ask your Field Office to initiate the FBI's Financial Fraud Kill Chain.
- Secret Service: https://www.secretservice.gov/contact/field-offices/

Step 6: Call the sending bank again to confirm that the recall request has been processed.

Step 7: Document your response using a Response Worksheet.

- Customize this ALTA Rapid Response Plan for Wire Fraud Incidents
- Customize a Response Worksheet (available in Excel or PDF)
- Assign each step to an appropriate person/entity
- Track progress through to completion or resolution
- Retain the Response Worksheet for future reference/update

Step 8: Consider contacting your insurance carrier(s) and outside legal counsel.

Step 9: Review your Incident Response Plan to determine if you need to update passwords, secure hardware, and review email logs to determine how and when email accounts were accessed.

Step 10: If funds were wired out of the U.S., hire an attorney in that country to help recover funds.