OLD REPUBLIC TITLE

Wire Fraud Rapid Response Plan

STEP 1

STEP 1 – Notify 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.
- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain (https://www.alta.org/news/news.cfm?20190131-Hit-by-Wire-Transfer-Fraud-Use-the-Kill-Chain-Process) if the amount of the wire transfer is $50,000 or above; the wire transfer is international; a SWIFT (www.swift.com) recall notice has been initiated; or the wire transfer has occurred within the last 72 hours.
- 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 2

Step 2 – File a complaint with the FBI's IC3 Center, visit www.ic3.gov and provide the following:

- 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.

STEP 3

STEP 3 – Report the incident to local law enforcement and contact your local FBI field office and provide the IC3 complaint number.

- Local Police/Sheriff: www.policeone.com/law-enforcement-directory
- FBI Field Office: www.fbi.gov/contact-us/field-offices
- Secret Service: www.secretservice.gov/contact/field-offices

STEP 4

STEP 4 – Inform all parties to the transaction and your support team.

- Notify the buyer, seller, real estate professionals, attorneys, underwriters, notaries, etc. using known, trusted phone numbers for verbal verification.
- Notify your Manager, Accounting, I.T., Legal Counsel and Underwriter.

STEP 5

STEP 5 – Review your Incident Response Plan.

Determine if you need to update passwords, secure hardware and review email logs to determine how and when emails were accessed. **Review email logs for *all* pending transactions using strict scrutiny to detect any other wire fraud attempts.**

STEP 6

STEP 6 – Consider contacting your insurance carrier(s) and outside legal counsel.

AgencyDriven™