



Fraud Notification Procedure

www.flta.org/CyberSecurity

PURPOSE: FLTA has established the following procedures for reporting suspected or detected fraud schemes and attacks. Along with how to document the results to help our industry recognize and avoid similar issues in the future.

PROCEDURES: The following steps are suggested when a fraudulent scheme or deceptive act has been detected, and are in no particular order.

Step 1. Report to I.T./Support Team: Notify your IT Professional Team immediately.

Step 2. Create a Fraud File: Collect all relevant documentation concerning the event in one file kept in a secure location.

- Timeline of events and, if applicable, any notes you feel may be relevant.
- Any evidence of the fraud or deception (i.e. emails, wire instructions, etc.)
- Any other relevant documentation concerning the fraud.
- All relevant contact information.

Step 3. Notify Banks: Call Banks for any accounts that were opened or used in connection with the scheme. Work with Bank to have account shut down and account holder's Tax ID number reported to Financial Crimes Enforcement Network (FinCen).

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](http://www.flta.org/file.cfm?name=FBI-FinancialFraudKillChain) (www.flta.org/file.cfm?name=FBI-FinancialFraudKillChain) if the amount of the wire transfer is \$50,000 or above; the wire transfer is international; a [SWIFT](http://www.swift.com) (www.swift.com) recall notice has been initiated; and 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 4. Report to the Appropriate Federal Agencies:

- Local Police/Sheriff: <https://www.policeone.com/law-enforcement-directory/>
- FBI Field Office: <https://www.fbi.gov/contact-us/field-offices>
- Secret Service: <https://www.secretservice.gov/contact/field-offices/>
- File a complaint with the FBI's Internet Crime Complaint Center (IC3). Visit www.ic3.gov 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](http://www.alta.org/file.cfm?name=HowToCopyEmailHeaders) (www.alta.org/file.cfm?name=HowToCopyEmailHeaders)
 - Any other relevant information that is necessary to support the claimant

Step 5. Inform the parties to the transaction: Notify buyer, seller, real estate agents, broker, attorneys, underwriter, notary, etc.) using known, trusted, phone numbers for verbal verification.

Step 6. Review your Written Incident Response Plan (WIRP) to determine if you need to update passwords, secure hardware, and review email logs to determine how and when email accounts were accessed.

Step 7. Notify Registrar of Domain. If a Spoofed Email is being used in connection with the scheme, contact the registrar who manages the registration of that domain name and report the abuse. Search <https://whois.net/> to locate Registrar.

Step 8. Contact your insurance carrier(s) and consider contacting outside legal counsel. If funds were wired out of the U.S., consider hiring an attorney in that country to help recover funds.

Step 9. (SPECIFIC TO WIRE FRAUD ONLY) Document your response using a Response Worksheet.

- Customize this [ALTA Rapid Response Plan for Wire Fraud Incidents](http://www.alta.org/file.cfm?name=ALTA-Rapid-Response-Plan-for-Wire-Fraud-Incidents) (www.alta.org/file.cfm?name=ALTA-Rapid-Response-Plan-for-Wire-Fraud-Incidents)
- Customize a Response Worksheet



- Excel Format (www.alta.org/file.cfm?name=Rapid-Response-Worksheet--Excel-Format)
- PDF Format (www.alta.org/file.cfm?name=Rapid-Response-Worksheet---PDF-Format)
- Assign each step to an appropriate person/entity.
- Track progress through to completion or resolution.
- Retain the Response Worksheet in your Fraud file for future reference/update.