

# ALTA Rapid Response Plan for Wire Fraud Incidents

## 10-step Guide on What to Do and Who to Contact

Information security and wire transfer fraud are critical topics for the land title insurance and settlement industry. Wire transfer fraud is a threat to every title operation regardless of size, location or years in business. ALTA's priority is helping you protect your systems, plan for a rapid response in case of an incident, and prepare your employees, clients and customers to be aware and vigilant.

This is why ALTA's Information Security Committee created a Rapid Response Plan. The plan outlines 10 steps that companies should follow if they've been hit by wire fraud. In addition, there's a worksheet to help you develop your own rapid response plan.

You can pull out this special section and post in your office to help educate staff about the rapid response plan. Digital files also are available at [alta.org/infosec](http://alta.org/infosec).



# ALTA Rapid Response Plan For Wire Fraud Incidents

## — RESPONSE WORKSHEET —

Date/time of incident \_\_\_\_\_

Date/time incident was discovered \_\_\_\_\_

Incident discovered by \_\_\_\_\_

Amount \_\_\_\_\_

Transaction affected (file number) \_\_\_\_\_

Client/parties affected \_\_\_\_\_

Systems/devices affected \_\_\_\_\_

Response coordinator \_\_\_\_\_

<b>Step 1</b>	<b>Alert company management</b> — Notes:	Assigned to:
<b>Step 2</b>	<b>Report to sending and receiving banks</b> — Notes:	Assigned to:
<b>Step 3</b>	<b>Report to law enforcement</b> — Notes:	Assigned to:
<b>Step 4</b>	<b>Confirm recall request was processed by sending bank</b> — Notes:	Assigned to:
<b>Step 5</b>	<b>Inform clients/parties affected</b> — Notes:	Assigned to:
<b>Step 6</b>	<b>Review Incident Response Plan for next actions</b> — Notes:	Assigned to:
<b>Step 7</b>	<b>Contact insurance carrier(s) and legal counsel</b> — Notes:	Assigned to:
<b>Step 8</b>	<b>Hire counsel in country where funds were wired</b> — Notes:	Assigned to:
<b>Step 9</b>	<b>Document your response</b> — Notes:	Assigned to:
<b>Step 10</b>	<b>File a complaint with the FBI</b> — Notes:	Assigned to:



# ALTA Rapid Response Plan for Wire Fraud Incidents

*Time is of the essence—every second and minute counts. Contact banks, transaction parties and law enforcement immediately upon discovery.*

## **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
- Others?

## **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.
- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain if the amount of the wire transfer is \$50,000 or above; the wire transfer is international; a SWIFT 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 3 Report Fraudulent Wire Transfers and Attempts to Law Enforcement.**

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

## **STEP 4 Call the sending bank again to confirm that the recall request has been processed.**

## **STEP 5 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 6 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 7 Consider contacting your insurance carrier(s) and outside legal counsel.**

## **STEP 8 If funds were wired out of the U.S., hire an attorney in that country to help recover funds.**

## **STEP 9 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 10 File a complaint with the FBI's Internet Crime Complaint Center (IC3).**

Visit [www.ic3.gov](http://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)
- Any other relevant information that is necessary to support the claimant