



## UNDERWRITING COMMUNICATION

Issued by

**First American Title Insurance Company**

**NC-2019-004 Alert**

**FROM:** Karl Knight, State Counsel for North Carolina

**DATE FILED:** March 13, 2019

### **Rapid Response Plan for Wire Fraud Incidents (Resource)**

**Purpose:**

This Alert is being sent to all agents and employees of First American Title Insurance Company doing business in the State of North Carolina. Attached please find a valuable resource entitled, "ALTA Rapid Response Plan for Wire Transfer Fraud Incidents<sup>3</sup>" and accompanying worksheet.

In the event guidance or resources are requested by one of your approved attorneys regarding a Wire Fraud Incident, please share the following "ALTA Rapid Response Plan for Wire Transfer Fraud Incidents<sup>3</sup>" and Worksheet, provided by the American Land Title Association.

Advance review of the procedures contained in this valuable resource may save time and money for any firm dealing with such an unfortunate incident.

**Contact Information for Questions:**

If you have any questions, please feel free to contact the State Office or email [tkknight@firstam.com](mailto:tkknight@firstam.com). Thank You.

**NOTE: This Bulletin is intended for use by title issuing offices, title insurance agents and approved attorneys of First American Title Insurance Company and any reliance by any other person or entity is unauthorized. Should you have any questions regarding this Bulletin, please contact your local First American underwriter.**

**PLEASE SHARE THIS BULLETIN WITH YOUR STAFF AND RETAIN AS PART OF YOUR  
PERMANENT REFERENCE MATERIALS.  
UNLESS OTHERWISE NOTED HEREIN, ALL OTHER UNDERWRITING  
COMMUNICATIONS APPLY.**

**© 2019 First American Financial Corporation and/or its affiliates. All rights reserved.**

## 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.  
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: <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/>

### 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) – [Learn how](#)
- Any other relevant information that is necessary to support the claimant

## ALTA Rapid Response Plan for Wire Fraud Incidents - Response Worksheet

<p><b>Date/Time of Incident:</b> _____</p> <p><b>Date/Time Incident was Discovered:</b> _____</p> <p><b>Incident Discovered By:</b> _____</p> <p><b>Amount:</b> _____</p> <p><b>Transaction Affected (File Number):</b> _____</p> <p><b>Client/Parties Affected:</b> _____</p> <p><b>Systems/Devices Affected:</b> _____</p> <p><b>Response Coordinator:</b> _____</p>	
<p><b>Step 1: Alert Company Management - Notes:</b></p>	<p><b>Assigned To:</b></p>
<p><b>Step 2: Report to Sending and Receiving Banks - Notes:</b></p>	<p><b>Assigned To:</b></p>
<p><b>Step 3: Report to Law Enforcement - Notes:</b></p>	<p><b>Assigned To:</b></p>
<p><b>Step 4: Confirm recall request was processed by Sending Bank - Notes:</b></p>	<p><b>Assigned To:</b></p>

<b>Step 5: Inform clients/parties affected - Notes:</b>	<b>Assigned To:</b>
<b>Step 6: Review Incident Response Plan for next actions - Notes:</b>	<b>Assigned To:</b>
<b>Step 7: Contact insurance carrier(s) and legal counsel - Notes:</b>	<b>Assigned To:</b>
<b>Step 8: Hire counsel in country where funds were wired - Notes:</b>	<b>Assigned To:</b>
<b>Step 9: Document your response - Notes:</b>	<b>Assigned To:</b>
<b>Step 10: File a complaint with the FBI - Notes:</b>	<b>Assigned To:</b>