

WHAT TO DO IF YOU ENCOUNTER *WIRE FRAUD*

Quickly consider this non-exclusive checklist of issues if Wire Fraud impacts your Agency.

Brought to you by:



1. CONTACT SENDING BANK IMMEDIATELY!

If funds have been sent in accordance with fraudulent wire instructions, contact the sending bank immediately upon discovery and ask the bank; 1) to attempt a wire recall due to fraud, and 2) to contact the corresponding recipient bank where the wire was sent.

3. NOTIFY THE POLICE

Notify the local police and make a report.

5. CONSULT WITH LEGAL REPRESENTATION

Consult with your legal representation. If applicable, check your E&O insurance for cyber fraud coverage, or a separate cyber fraud coverage policy, and put them on notice of the breach and potential loss.

7. NOTIFY THE PARTIES

Verbally notify the parties to the transaction via known, trusted telephone numbers that electronic communication may have been compromised by unauthorized parties. Recommend all parties review email account security, including changing email passwords and conducting security reviews of computers and networks. All further communications regarding the transaction, particularly involving money, should be conducted via phone calls to known, trusted telephone numbers until the source of the compromise can be identified and mitigated.

2. CONTACT THE RECIPIENT BANK

Contact the recipient bank yourself also, advise them of the situation, and request that they freeze the recipient account.

4. NOTIFY THE FBI

Contact your local FBI office and file a Business Email Compromise complaint, regardless of the dollar loss, at www.IC3.gov.

6. WORK WITH YOUR IT DEPARTMENT

Have your IT Department or external IT consultant check your server and computer for compromise.



Please feel free to contact the Chicago Title, Commonwealth Land Title and Fidelity National Title

This Notice is not intended to provide legal or professional advice. If you have questions, please consult with a lawyer.