WIRE FRAUD CHECKLIST

You suspect or know that money has been wired to the wrong account. Likely, your initial concern is how to get the misdirected money back. While there is no guarantee that the misdirected funds can be returned, here are five recommended steps to take to maximize the likelihood of recovering the misdirected money.

Recommended Steps to Attempt Recovery of Misdirected Funds

1 ❑ **Contact the sending bank (the bank from which the money was wired).**

- ❑ Did the sending bank file a SAR (Suspicious Activity Report)?
- ❑ Did the sending bank provide a copy of the filed SAR?

2 ❑ **Contact the receiving bank (the bank to which the money was wired).**

3 ❑ **Contact the closest Secret Service office.**

4 ❑ **Contact the person/entity the funds were intended.**

5 ❑ **Contact your cyber insurance carrier.**

Ideally, you were able to recover the misdirected funds. If so, skip to "Steps to Help Prevent This From Happening Again." If not, there is still a chance to mitigate the loss of the misdirected funds.

There may be a dispute between the issuing party and the intended receiving party over which party is at fault, and therefore which side bears responsibility for the misdirected funds. One way to help resolve this dispute is for each party to conduct a forensic investigation.

A party may also have access to insurance. Depending on the available coverage and the circumstances surrounding the misdirection of funds, insurance may cover some or all the loss.

It is also prudent to search for outstanding wire payments – both wire payments that have been issued and that have yet to be received – to validate those payments are going to the intended recipients.

WIRE FRAUD CHECKLIST

Steps to Mitigate Losses

1. ❑ **Expire all logged in sessions and reset all email passwords**
2. ❑ **Conduct a forensic investigation**
   - ❑ Did the forensic investigation reveal unauthorized activity in your email environment?
   - ❑ Did the forensic investigation reveal NO unauthorized activity in your email environment?
3. ❑ **Did the individual/entity that was to receive the wire conduct a forensic investigation?**
   - ❑ Did the forensic investigation reveal unauthorized activity in their email environment?
   - ❑ Did the forensic investigation reveal NO unauthorized activity in their email environment?
4. ❑ **Did you search for any outstanding wire payments (ones that you made)?**
   - ❑ Did you contact the identified payors to confirm the wire instructions?
5. ❑ **Did you search for any outstanding wire payments (ones that you expect to receive)?**
   - ❑ Did you contact the identified payors to confirm the wire instructions?

Steps to Help Prevent This From Happening Again

1. **Incorporate language in your email signature/invoices that your organization will not change wiring instructions via email.**
2. **Incorporate language in your email signature/invoices that before an individual issues a wire transfer that individual must call: (1) a known individual; (2) using a previously used number; (3) to confirm the wire instructions.**
3. **Update your contracts to require a third-party issuing wire payments to: (1) confirm the wire instructions before sending a wire; (2) cover 100% of the misdirected funds if the third-party does not confirm wire instructions.**