Where the Money Vanishes: How Construction Firms Can Combat wire Fraud and Recover Insurance Proceeds

By Luma S. Al-Shibib and Caroline Levine

You receive an email from a trusted supplier asking for payment of an unpaid invoice. The email appears like your usual correspondence and includes a typical invoice you receive from the supplier. It mentions that the supplier has a new account at a different financial institution and provides different wire instructions. Since the email appears legitimate, you wire the money, however, you do not receive any confirmation of receipt from the supplier like you always do. When you call the supplier and ask if it received your payment, the supplier has no idea what you are talking about. You then realize you have been duped by a cybercriminal pretending to be your supplier.

This scenario – and ones similar to it – have become increasingly common in the construction industry. The complex chain of contractors, owners, suppliers, and vendors involved in construction projects provides many potential targets for cyber fraud. In fact, the construction industry was the third most targeted industry worldwide for cyberattacks in 2024.

The most common type of cyber fraud in the construction industry is Funds Transfer Fraud. It occurs when a cybercriminal makes a seemingly legitimate request for a money transfer and manipulates you or your financial institution into sending funds to a fraudulent account. The use of AI has increased the frequency and sophistication of these types of attacks.

In many cases, financial losses can be irreversible if the scheme is not promptly discovered and reported to authorities. Law enforcement and your bank may be able to electronically trace and "claw back" some or all of the stolen funds – but only if reported within the first 72 hours of the transfer. Beyond that initial window of time, however, victims are unlikely to recover their transferred funds because cybercriminals quickly convert the money into cryptocurrency or move it through multiple bank accounts.

Funds Transfer Fraud Insurance Coverage May Help Mitigate Your Losses in the Event of a Cyber Fraud Incident

If you do experience cyber fraud, insurance may respond and cover some or all of your losses. A broker well-versed in the construction industry can advise you about the types of policies or coverages needed to protect against Funds Transfer Fraud. Typically, coverage for cyber fraud is available under crime and cyber policies – although other policies may also offer coverage. If you suffer a loss, ask your broker to provide notice of the claim under all your potentially applicable insurance policies.

Because policies can vary significantly in their terms and exclusions, it is critical for policyholders to be aware of what their specific policies say.

Funds Transfer Fraud coverage, which is usually found in crime policies but may also exist under cyber policies, insures against losses stemming from wire fraud. In typical cases, a fraudster impersonates a legitimate party with which you conduct business, such as a vendor or supplier, and tricks you into wiring or transferring money to the fraudster's account. In most of these scenarios, the cybercriminal will use social engineering techniques, such as theft of a customer's or supplier's email credentials, to execute its fraudulent scheme.

Policies providing coverage for Funds Transfer Fraud may include various conditions. Insurance companies seeking to reduce their liability may raise noncompliance with policy conditions as a defense to coverage. To maximize recovery, you must understand any conditions to coverage. For example, before making the wire transfer, your company may need to verify the wire transfer request by calling the vendor or supplier. Usually, the insurance policy will require that the verification call is made to a previously agreed-upon telephone number on file for the vendor or supplier. Additionally, you may need to keep a contemporaneous record of the verification call and submit this document as part of the insurance claim submission. Furthermore, any changes you make to a customer, vendor, or client's wire instructions may require a written request from the customer, vendor, or client on their letterhead, and reference their account number or passcode. Also, you may have to observe a waiting period before you can wire money after making changes to the bank account information in a customer, vendor or client's file. While these are some of the common conditions found in policies covering funds transfer fraud, your policy may have different conditions.

Your insurance company may argue that it does not have to cover your claim if you fail to satisfy the conditions of the policy. This underscores the importance for businesses – including those in the construction industry – to read their policies, understand any requirements to coverage, and incorporate those requirements into their standard operating procedures. Remember that every policy is different so not all conditions will be the same across different policies or different coverages.

Additionally, your loss may trigger coverage under more than one provision in your policy and may implicate several different policies. For example, computer fraud coverage, typically found in crime policies, offers broad coverage for losses resulting directly from fraud through the unauthorized use of a computer, and some courts have held that computer fraud coverage responds to cover losses from cyber crimes – including wire transfer fraud. Also, social engineering coverage under either your cyber or crime policy may also respond to your claim; however, social engineering coverage may have a separate sublimit that is lower than the policy's per claim limit. Thus, it is important to discuss your claim with your broker and ask your broker to provide notice of the loss under all potentially implicated policies.

Conclusion

Cyber fraud poses a significant and growing threat to the construction industry. The combination of high-value wire transfers, complex project teams, and significant email and computer reliance for payment and project management makes construction companies particularly vulnerable to Funds Transfer Fraud. Your insurance policies provide a meaningful way to mitigate your losses, but your ability to recover for your losses largely depends on policy language.

To maximize coverage, you should

1. Review your insurance policies to understand their coverages and requirements.
2. Incorporate any policy requirements into your standard business procedures (for example, call back verification for wire transfers).
3. Train your employees to be aware of what fraudulent requests look like and institute strong internal controls and verification requirements.
4. Contact the FBI and local authorities ASAP to report the cybercrime. In some cases, funds can be traced and recouped if the crime is reported early enough.
5. Ask your broker to provide notice of your loss under all potentially applicable policies.

Author

Luma S. Al-Shibib / *lal-shibib@andersonkill.com*
Luma is a shareholder in Anderson Kill's New York office. She focuses her practice on insurance recovery for corporate policyholders, with an emphasis on cyber liability insurance, crime insurance, directors & officers liability insurance, and otheer claims-made professional liability insurance. She is Co-Chair of the firm's Cyber Insurance Recovery Group.

Caroline Levine / *clevine@andersonkill.com*
Caroline is an attorney in Anderson Kill's New York office where she focuses her practice on insurance recovery. She is a member of the firm's Restaurant, Retail, and Hospitality Group.

ANDERSON KILL

Known as the Policyholder Powerhouse™, Anderson Kill is a pioneer in insurance coverage litigation: we have more experience in litigating, trying and settling insurance coverage disputes than any other law firm. As the only four-time winner of Business Insurance's **Legal Team of the Year**, our firm has an extraordinary record of obtaining insurance coverage for policyholders in connection with all manner of insured losses. The firm has offices in New York, NY; Boston, MA; Los Angeles, CA; Newark, NJ; Philadelphia, PA; Stamford, CT; and Washington, D.C.