Strategies For Wire Fraud Prevention As Risk Is On The Rise

By **Casey Jennings** (December 20, 2023)

Casey Jennings

We have observed a troubling trend in recent months of criminals using fraudulent wire transfer schemes to target financial institutions, or FIs. This trend is increasingly affecting investment managers and funds, nonbank fintech companies, and crypto custodians and their clients, as well as customers and investors.

Below, we discuss how these schemes operate and steps that FIs can take to mitigate this increasing risk.

Attack Patterns

In these attacks, the primary goal of a fraudster is to prompt either a company or its customers to initiate a wire transfer to a bank account controlled by the fraudster.[1] Fraudulent wire transfer schemes can take any number of forms, including:

- The fraudster compromises an FI's systems and, posing as the FI, directly instructs the FI's bank, broker, custodian or other financial institution to wire funds to a bank account controlled by the fraudster.
- The fraudster compromises the FI's systems and, posing as the FI, directs clients to wire funds to a bank account controlled by the fraudster.
- The fraudster compromises an FI's systems and, posing as a company executive, directs an employee to wire funds to a bank account controlled by the fraudster.
- The fraudster compromises a customer's systems or identity and directs the FI to wire funds from the client's account at the FI to a bank account controlled by the fraudster.

Tactics frequently employed by fraudsters include:

- Urgent requests for wire transfers;
- Requests to send wire transfers to unfamiliar accounts;
- Fraudulent invoices;
- Links and attachments in emails; and
- Emails requesting verification of accounts or payments.

These attacks are often perpetrated by sophisticated criminals, and many are conducted by state actors or state-backed organizations.

While many of these attacks do not require public reporting under state data breach notification laws, which tend to be somewhat narrow, several recent public examples illustrate the risks.

On Nov. 18, 2022, the U.S. Department of Justice announced charges against 10 individuals in connection with multiple large wire fraud schemes, resulting in a total loss exceeding

$11.1 million.[2]

Impersonating legitimate business partners, these fraudsters emailed Medicare, state Medicaid programs and private health insurers, among others, with fraudulent wire transfer requests. In one instance, public and private health insurance programs were sent emails from accounts resembling those associated with actual hospitals, containing instructions to wire future payments to different accounts controlled by the fraudsters.

Another recent $5.8 million wire fraud scheme[3] was detailed by the U.S. Attorney's Office for the Southern District of New York in an indictment unsealed June 7.[4]

By impersonating legitimate business contacts by email, fraudsters were able to convince a hospital, labor union, law firm, real estate company and logistics company to wire a total of $5.8 million into their bank accounts.

In a similar case, Elkin Valley Baptist Church — which had spent a decade collecting $1.5 million to fund the building of a new worship center — in November 2022 received a legitimate wire transfer request from their builder for the first half of the payment.

That request was quickly followed by another email nearly identical to the first, even including the previous email thread. However, this email contained different transfer instructions, and a church representative sent nearly $800,000 to the fraudulent bank account.[5]

Potential Consequences

The consequences of a fraudulent wire transfer can be dire. Wire transfers are a preferred attack vector because under Article 4A of the Uniform Commercial Code, which governs wires, there are limited transaction reversal rights.[6]

By contrast, automated clearing house transfers are subject to a greater number of transaction reversal rights, which can sometimes shift the liability for the fraud from the defrauded company to one of the banks involved in the transaction.[7]

Typically, wire transfers cannot be reversed more than 24 hours following the transfer. The fraudster will usually abscond with the funds as soon as the transfer settles, and it can be very difficult to trace the funds for recovery purposes. Once the money is gone, it's usually gone for good.

Prevention Measures

The first prevention measure an FI can take is to make wire transfer fraud prevention a priority. Implement a robust cybersecurity policy that educates employees on wire transfer fraud risks and best practices to prevent wire transfer fraud. Employees should be made familiar with the types of scams and tricks fraudsters frequently use, and how to properly identify fraudulent requests.

Educate your employees on your wire transfer verification process. It can also be helpful to test the effectiveness of your cybersecurity policy by sending fake phishing emails and evaluating your company's response.

Mechanically, the best way for an FI to defend against these attacks is to introduce friction into the wire transfer process as a circuit breaker. This has the unfortunate effect of

reducing efficiency, but fraudsters rely on efficiency to get in and get out before anyone knows what has happened.

The easiest way to introduce a circuit breaker into the wire transfer process is to integrate a telephone call requirement for each transfer (or each transfer above a certain dollar threshold). For each wire transfer you send, confirm via telephone call — i.e., speak to another human being — the amount and account number to which you are wiring funds.

For each wire transfer you request from a customer or vendor, inform the counterparty that you will provide or confirm transfer instructions via telephone call and instruct them not to wire funds without telephone confirmation.

Additionally, telephone call verification should be done using a reliable phone number, one you have already used to contact the counterparty in the past. Never use any contact information provided in the email itself.

Another recommended circuit breaker is to require the involvement of more than one person in your organization's wire transfer process. A multiple-person wire process has many benefits, such as having another pair of eyes reviewing the request and potentially identifying it as fraudulent.

It also prevents the person who receives the request from falling for the common tactic of sending requests marked as urgent. An example would be not allowing the person who receives the request to send the wire transfer.

If your organization processes emailed wire transfer requests, carefully scrutinize the email address of the sender. A frequent tactic used by fraudsters is to send a wire transfer request from an email address that is almost identical to a legitimate email address, but contains a small, difficult-to-notice variation.

For example, if a legitimate email address is lastname@lawfirm.com, a fraudster may send an email from lastname@lawfrim.com.

Larger organizations may be able to build more automated means of confirmation, such as one-time pass codes using two-factor authentication or a requirement to answer challenge questions.[8] However you choose to do it, the key is to interpose a circuit breaker of some kind.

Response Procedures

Depending on the circumstances, you may need to alert law enforcement,[9] your regulator[10] and affected customers[11] if you have been the victim of a wire transfer fraud. You can immediately file a report with the FBI[12] using the IC3[13] system. Quickly contact the bank to which the money was wired and inform them of the situation.

Fraudsters almost always begin transferring or withdrawing money immediately, so it is important to contact both banks before the money becomes irretrievable. On Dec. 14, 2022, a Denver woman was able to recover $91,000 out of a total of $97,000 by quickly contacting Wells Fargo — the bank that received the stolen funds — and explaining the situation.[14]

Wells Fargo was able to freeze the fraudulent account in time before the fraudster transferred the funds.

You may also need to engage a third-party forensic specialist to determine the attack vector and remediate any security vulnerabilities. An engagement made through an outside law firm should protect any communications, findings or reports produced by the specialist through the attorney-client privilege.

As always, consult your own internal policies and procedures for responding to a security issue. Regulators do not expect data security perfection from FIs, but they do expect FIs to follow their internal procedures to a T.

Casey Jennings is counsel at Seward & Kissel LLP.

[1] What is a wire transfer?, Consumer Financial Protection Bureau, Oct. 17, 2022, https://www.consumerfinance.gov/ask-cfpb/what-is-a-wire-transfer-en-1163/.

[2] 10 Charged in Business Email Compromise and Money Laundering Schemes Targeting Medicare, Medicaid, and Other Victims, Dep't. of Justice Office of Public Affairs, Nov. 18, 2022, https://www.justice.gov/opa/pr/10-charged-business-email-compromise-and-money-laundering-schemes-targeting-medicare-medicaid.

[3] Six Defendants Arrested for Multimillion-Dollar Wire Fraud and Money Laundering Scheme, United States Attorney's Office — Southern District of New York, June 7, 2023, https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multimillion-dollar-wire-fraud-and-money-laundering-scheme.

[4] Sealed Indictment, U.S. v. Ndama-Traore et. al, 2023 U.S. Dist. LEXIS 108669 (S.D.N.Y. June 22, 2023), https://www.justice.gov/media/1297856/dl?inline.

[5] Associated Press, N. Carolina church says it lost nearly $800K in email scam, Yahoo! Finance, Jan. 28, ,2023, https://nz.finance.yahoo.com/news/n-carolina-church-says-lost-213905294.html?guccounter=1.

[6] U.C.C. — Art. 4A — Funds Transfer (2012), Legal Information Institute, https://www.law.cornell.edu/ucc/4A.

[7] What is an ACH?, Consumer Financial Protection Bureau, Aug. 27, 2020, https://www.consumerfinance.gov/ask-cfpb/what-is-an-ach-en-1065/.

[8] Office of Compliance Inspections and Examinations, Cybersecurity: Safeguarding Client Accounts against Credential Compromise, Securities and Exchange Commission, Sept. 15, 2020, https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf.

[9] Cybersecurity Unit, U.S. Dep't. of Justice Criminal Division, Aug. 11, 2023, https://www.justice.gov/criminal/criminal-ccips/cybersecurity-unit.

[10] Cybersecurity, U.S. Securities and Exchange Comm'n, July 31,

2023, https://www.sec.gov/securities-topics/cybersecurity.

[11] Saniuk-Heinig, Cheryl, State Data Breach Notification Chart, IAPP, https://iapp.org/resources/article/state-data-breach-notification-chart/.

[12] Federal Bureau of Investigation, https://www.fbi.gov/.

[13] Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, https://www.ic3.gov/Home/ComplaintChoice.

[14] Allen, Jaclyn, Denver woman stops fraudulent wire transfer just in time. Here's how she did it., Denver7, April 12, 2023, https://www.denver7.com/news/contact-denver7/denver-woman-stops-fraudulent-wire-transfer-just-in-time-heres-how-she-did-it.