

# Never Trust, Always Verify: How to Avoid Wire Fraud



**Alex Lesch**  
Partner,  
Investment Strategy  
& Risk Management

**Kathleen Schau**  
Vice President,  
Investment Strategy  
& Risk Management

## KEY TAKEAWAYS

- US cybercrime losses have more than tripled since 2019, topping \$12.5 billion, according to the FBI, with investment scams and business email compromise the costliest frauds
- The golden rule of wire fraud prevention is to never trust the source of a request for funds – always verify
- Even if an organization's systems and processes are secure, it's still possible to fall victim to a deceit if a counterparty has been compromised

The threat of cybercrime is significant and growing. Reports of cybercrime by the American public rose 10% to a record 880,413 in 2023, according to the Federal Bureau of Investigation (FBI), generating potential losses in excess of \$12.5 billion, a 22% surge from the previous year.<sup>1</sup>

Monetary losses more than tripled as the number of complaints nearly doubled in the five years through 2023, the FBI's Internet Crime Complaint Center (IC3) says.<sup>2</sup> But that likely masks the true scale of the problem, as the agency estimates that only about 20% of incidents are reported.

Losses to investment scams rose 38% to \$4.57 billion in 2023, while business email compromise (BEC) was the second costliest cybercrime, accounting for \$2.9 billion in reported losses.<sup>3</sup>

We view cyber fraud prevention as a collective effort at Adams Street, where IT and Cybersecurity risk is one of six pillars in our operational due diligence framework. Governance, Compliance, Service Providers, and Reputational Risk are other pillars, while the final one, Financial Management & Reporting, incorporates due diligence procedures to assess and confirm processes around cash controls and a manager's ability to prevent the misappropriation of financial assets.

Constant vigilance is required to stay ahead of emerging schemes. Strengthening financial controls and cybersecurity tools to minimize vulnerabilities is a permanent focus of our due diligence reviews that incorporate sharing best practices with managers and highlighting how things can go wrong.

## Wire Fraud is a Risk for Everyone

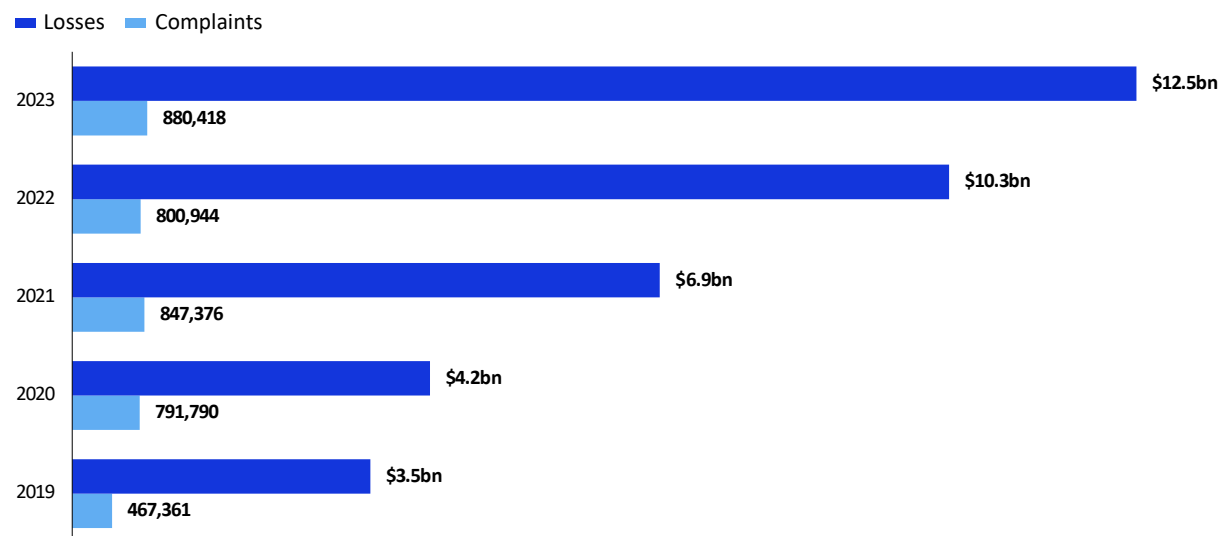
Wire fraud is a form of cybercrime that is a constant discussion topic among our teams. Wire fraud, which often presents itself as a financial and treasury management risk, can be mitigated by enforcing strong cash controls—multiple levels of review for payment requests, authorization, and independent confirmation of wire instruction details.

But organizations can still fall victim and send cash to a bogus account even when protocols are followed. This could be caused by a manual override in a critical detection step, or because a team has been targeted by phishing, spoofing, or deepfake scams.

Phishing campaigns are increasingly sophisticated, and cybercriminals can now mimic legitimate communication using artificial intelligence (AI). While tools such as email, text, instant messaging, video conferencing, and mobile banking have improved communication speed and efficiency, they also increase susceptibility to financial crime, especially wire fraud.

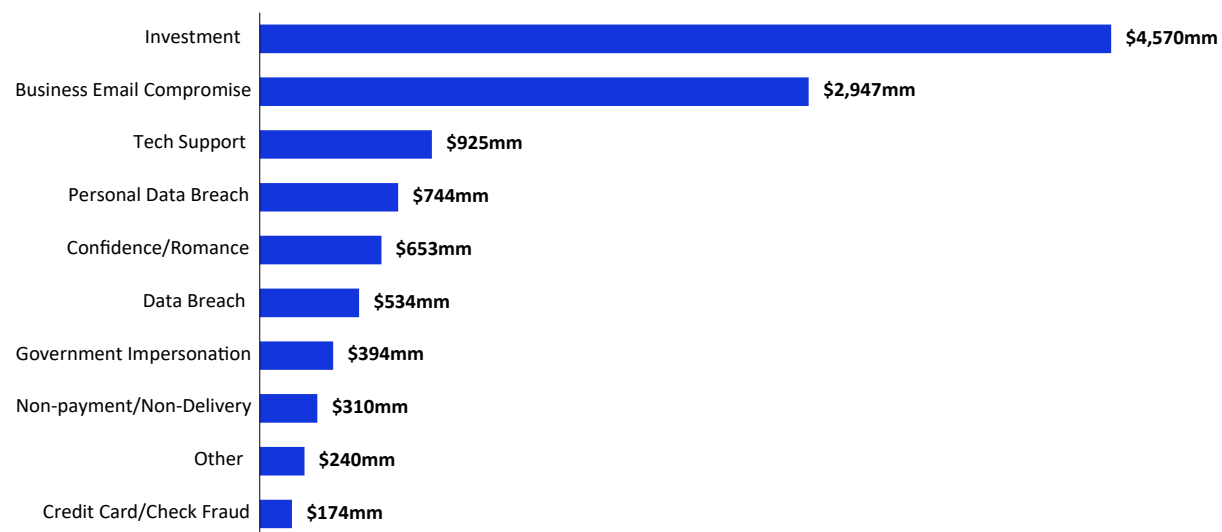
---

### Cybercrime Losses and Complaints (2019-2023)<sup>4</sup>



---

### Top 10 Cybercrime Losses by Complaint Type (2023)<sup>5</sup>



# Wire Fraud in Private Markets

In private markets, BEC is the primary threat leading to misdirected wire transfers. Cybercriminals are aware of the large sums transacted in private equity. The total value of global private equity deals reached a projected \$2 trillion in 2024,<sup>6</sup> excluding an additional \$600 billion in capital draws and \$700 billion in distributions in the first half of 2024.<sup>7</sup> Poor oversight and controls in even a small fraction of transactions could result in many millions of dollars being funneled to criminals.

## Cybercriminal Playbook





BEC scams typically occur when cybercriminals steal email credentials through malware or phishing attempts. They may also employ phishing emails that appear to be from known counterparts such as vendors, investors, portfolio companies, or financial institutions. Sophisticated schemes can lure victims to websites designed to capture their credentials.

So even if an organization’s systems and processes are secure, it’s still possible to fall victim to a BEC scam if a counterparty’s email system has been compromised. The proliferation of AI technology, such as audio deepfakes, further complicates the situation. Cybercriminals now use AI-generated voices to impersonate known contacts and to bypass typical detection methods.

---

### Wire Fraud Methods<sup>8</sup>

Cybercriminals use a variety of methods to conduct wire fraud. These include:

	<b>Malware</b>	Occurs when a user opens an email or clicks on a link that redirects to a website that downloads malware and infects the computer operating system. Criminals can also send malware through removable media, such as a USB flash drive. After the removable media is inserted into a computer drive, criminals can gather user credentials to gain access to payments systems.
	<b>Phishing</b>	Occurs when criminals send emails that appear to be sent from a known company or vendor, such as a bank. The criminal asks the user to reply to the email or visit a website that looks similar to the company’s domain and submit a username, password, account number or other personal information.
	<b>Voice Phishing and SMS Phishing</b>	Use live or automated calls (vishing) or text messages (SMShing) to intimidate callers into providing personal information by threatening to close or freeze their bank accounts. The personal information is used to gain access to payment systems or take over accounts.
	<b>Business Email and Email Compromise</b>	BEC or email account compromise (EAC) occurs when cybercriminals use stolen credentials, look-alike domains, spam or phishing to gain access to an email account. Cybercriminals may impersonate a known vendor or C-suite executive, such as the chief executive officer, and direct another employee to transfer funds to a fraudulent account.

## Three Rules of Wire Fraud Prevention: Verify, Verify, Verify

There are many ways cybercriminals can target organizations with BEC scams. A finance team might receive wire instructions with altered banking details from a seller's compromised email that a bad actor has intercepted. If no follow-up call is made to verify the details, fraud could result.



**Proactive measures that firms implement to safeguard against wire fraud and cyber threats should involve a combination of technology, people, and processes. Multilayered strategies help organizations minimize risk**

The same applies to variants of the BEC fraud. If a vendor sends a payment request with new wire instructions from an email that appears to be legitimate, the recipient should assume it's a spoof and seek verbal confirmation to avoid a fraudulent payment.

The most common factor to becoming a victim of wire fraud is not independently verifying new or changes to wire instructions. The human and manual element of verifying payment instruction is critical to the cash control process.

## Prevention Strategies

Proactive measures that firms implement to safeguard against wire fraud and cyber threats should involve a combination of technology, people, and processes. Multilayered strategies help organizations minimize risk, enhance security protocols, and ensure financial transactions are properly verified and protected from malicious actors.

A checklist should include:

### **CYBERSECURITY AND INTERNAL CONTROLS**

- Strong cybersecurity measures, such as multifactor authentication, spam filters, and network access controls.
- Training employees to recognize phishing attempts and suspicious communications.
- Implementing robust internal controls around cash management, including independent verification for wire transfers.

### **INDEPENDENT VERIFICATION**

- Always verify wire instructions through a separate communication channel, not just email and preferably with someone other than the one making the request.
- Attempt to confirm wire instructions through verbal communication or video calls.

### **RED FLAGS**

- Exercise caution when wire instructions change, involve overseas accounts, or include last-minute payment requests.
- Pay attention to unusual email addresses, language inconsistencies, or requests for secrecy and urgency.



## **Cyber Insurance Is Not a Safety Net**

Cyber insurance coverage is usually capped at \$5 million or less, so that it often doesn't fully indemnify a victim for large wire fraud losses. High deductibles and exclusions for things like social engineering or email spoofing can further limit a policy's effectiveness. Organizations need to understand their coverage, as policies typically support investigation and remediation, not reimbursement for financial losses.

## **Guilty Until Proven Innocent**

While IT security plays a crucial role in preventing and identifying fraud, human vigilance is also essential. In the words of Mark Lutostanski, a Principal in Client Operations at Adams Street who oversees cash management as Director of Private Equity Middle Office, "all wire instruction changes are regarded as potentially fraudulent, resulting in a 'guilty until proven innocent' mindset."

Implementing these strategies can significantly reduce the likelihood of becoming a victim of wire fraud. When properly trained, employees can become an organization's strongest defense. ■

1. [Federal Bureau of Investigation Internet Crime Report 2023](#)
2. Ibid
3. Ibid
4. Ibid
5. Ibid. Loss estimates comprise only those losses reported to the FBI via the Internet Crime Complaint Center and do not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. There are instances where entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate.
6. McKinsey & Company [Global Private Markets Report 2025: Private equity emerging from the fog](#), February 13, 2025
7. McKinsey & Company [Global Private Markets Report 2025: Private equity emerging from the fog](#), February 13, 2025, Page 21, Exhibit 14
8. J.P. Morgan Chase, [Identifying and Responding to Wire Fraud Attacks](#) Page 3

## LEADING WITH FORESIGHT™

**Adams Street Partners** is a global private markets investment manager with investments in more than 30 countries across five continents. The firm is 100% employee-owned and has \$62 billion in assets under management across primary, secondary, growth equity, credit, and co-investment strategies. Adams Street strives to generate actionable investment insights across market cycles by drawing on over 50 years of private markets experience, proprietary intelligence, and trusted relationships. Adams Street has offices in Austin, Beijing, Boston, Chicago, London, Menlo Park, Munich, New York, Seoul, Singapore, Sydney, and Tokyo, and Toronto. [adamsstreetpartners.com](https://adamsstreetpartners.com)

---

**Important Considerations:** This information (the “Paper”) is provided for educational purposes only and is not investment advice or an offer or sale of any security or investment product or investment advice. Offerings are made only pursuant to a private offering memorandum containing important information. Statements in this Paper are made as of the date of this Paper unless stated otherwise, and there is no implication that the information contained herein is correct as of any time subsequent to such date. All information has been obtained from sources believed to be reliable and current, but accuracy cannot be guaranteed. References herein to specific sectors, general partners, companies, or investments are not to be considered a recommendation or solicitation for any such sector, general partner, company, or investment. This Paper is not intended to be relied upon as investment advice as the investment situation of individuals is highly dependent on circumstances, which necessarily differ and are subject to change. The contents herein are not to be construed as legal, business, or tax advice, and individuals should consult their own attorney, business advisor, and tax advisor as to legal, business, and tax advice. In no event shall Adams Street or any of its employees or affiliates be liable for any use of, for any decision made or action taken in reliance upon or for any inaccuracies or errors in, or omissions from, the information in this material. Readers are responsible for determining how to best protect themselves against cyber threats, for selecting the cybersecurity best practices that are most appropriate to their needs and Adams Street assumes no responsibility or liability whatsoever to any person in respect of such matters. Past performance is not a guarantee of future results and there can be no guarantee against a loss, including a complete loss, of capital. Certain information contained herein constitutes “forward-looking statements” that may be identified by the use of forward-looking terminology such as “may,” “will,” “should,” “expect,” “anticipate,” “estimate,” “intend,” “continue,” or “believe” or the negatives thereof or other variations thereon or comparable terminology. Any forward-looking statements included herein are based on Adams Street’s current opinions, assumptions, expectations, beliefs, intentions, estimates or strategies regarding future events, are subject to risks and uncertainties, and are provided for informational purposes only. Actual and future results and trends could differ materially, positively or negatively, from those described or contemplated in such forward-looking statements. Moreover, actual events are difficult to project and often depend upon factors that are beyond the control of Adams Street. No forward-looking statements contained herein constitute a guarantee, promise, projection, forecast or prediction of, or representation as to, the future and actual events may differ materially. Adams Street neither (i) assumes responsibility for the accuracy or completeness of any forward-looking statements, nor (ii) undertakes any obligation to update or revise any forward-looking statements for any reason after the date hereof. Also, general economic factors, which are not predictable, can have a material impact on the reliability of projections or forward-looking statements. Adams Street Partners, LLC is a US investment adviser governed by applicable US laws, which differ from laws in other jurisdictions.