Global Data Privacy and Security Team

I Already Wired You The Money! I think… Wire Transfer Fraud At A Glance

Businesses are increasingly falling victim to wire fraud scams – sometimes referred to as "man-in-the-email" or "business email compromise" scams. Although there are multiple variants, a common situation involves an attacker gaining access to the email system of a company, or the company's vendor, and monitoring email traffic about an upcoming transaction. When it comes time to submit an invoice or a payment, the attacker impersonates one of the parties and sends wire instructions asking that payment be sent to the attacker's bank account.

Wire fraud scams often victimize two businesses – the business that expected to receive payment, and the business that thought that they had made payment. The scam can cause significant contractual disputes between the victims as to who should bear the loss.

The number of businesses victimized by wire transfer fraud. [1]	The amount of money lost in the US due to wire transfer fraud.[1]	Percentage of businesses that were the subject of attempted or actual wire transfer fraud.[2]
2,126	**$179** MILLION	**14%**

Steps to help avoid wire fraud scams:

- ✓ Avoid free web-based email systems to transact business.
- ✓ Enable multi-factor authentication to log into all email systems.
- ✓ Require employees to select unique and strong passwords or pass phrases.
- ✓ Require employees to change email passwords frequently.
- ✓ Require multi-factor authentication (e.g., email and telephone call) when receiving initial payment information.
- ✓ Require multi-factor authentication when receiving a request to change payment information.
- ✓ Send a confirmatory letter or email (not using the "reply" feature in email) concerning any request to change payment information.
- ✓ Delay payment in connection with any request to change payment accounts or request to make payment to a foreign bank account.
- ✓ Review any request received by email to change payment account for signs that the email may be from a third party.
- ✓ Provide clear instructions to business partners concerning how payment information should be communicated.

If you are victimized by wire fraud:

- ✓ Consider notifying the receiving bank and request that a freeze be placed on any remaining funds.
- ✓ Consider notifying law enforcement.
- ✓ Investigate whether your email system may have been compromised.
- ✓ Ask business partners to investigate whether their email systems may have been compromised.

[1] Federal Bureau of Investigation, Alert No. I-012215-PSA (dated Jan. 22, 2015) (time period for reporting 10/1/2013 – 12/1/2014).
[2] Association for Financial Professionals, 2014 AFP Payments Fraud and Control Survey Report of Survey Results (Apr. 2014) at 6 (reporting on 2013 data).

For more information on data breach litigation or to subscribe to the Bryan Cave Plaintiff Troll Alert contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

Jena M. Valdetero
Partner
jena.valdetero@bryancave.com
161 North Clark Street, Suite 4300
Chicago, IL 60601-3315
phone: 312 602 5000

BRYAN CAVE