WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Wire-Fraud, Data Breach, and Phishing: A Live Action Role Play for In House Counsel

Written By Angela P. Doughty, CIPP/US, AIGP (apd@wardandsmith.com) **and X. Lightfoot** (xlightfoot@wardandsmith.com)

April 2, 2024


At the recent In-House Counsel Seminar, three Ward and Smith attorneys presented a realistic role play response to an incidence of wire fraud, addressing red flags associated with fraudulent communications, corporate incident response planning, and determining who bears responsibility for missing funds.

The attorneys led the discussion around the nuances of managing a cyber security incident, cyber-insurance, recommended prevention measures and training courses, the difference between an incident and a breach, and notification obligations.

The session leveraged the firm's signature live-action role-playing (LARPing) technique to guide participants through a hypothetical scenario involving The Dapper Dashers, a family owned and operated courier service based in North Carolina with 13 employees, and Vista Ridge, a pharmaceutical company with 300 employees that is also based in North Carolina.

The discussion was led by Richard J. Crow, a business and tax attorney with extensive experience representing small and large companies with business organization, corporate governance, contract negotiations and drafting. It featured insights from Mayukh Sircar, a cybersecurity, data privacy, and technology attorney, and Paul Fanning, who leads the creditors' rights practice and is certified by the American Board of Certification and the North Carolina State Bar as a Board Certified Specialist in business and consumer bankruptcy law.

Case of the Misdirected Payment

Crow began by describing how a Dapper Dashers employee, "Hunter from accounts receivable," learned two payments from Vista Ridge totaling $96,000 were missing. Hunter noticed this was unusual for Vista Ridge, which had a long history of on-time payments through wire transfers. He immediately reached out to his colleague at Vista Ridge, who was confident the payment was sent in a timely manner.

Crow asked the seminar participants for ideas on possible next steps. Responses included calling the FBI, calling Ward and Smith, asking for payment details, and requesting wire transfer confirmation.

“Before assuming the worst, panicking or threatening to sue, it’s a good idea to contact employees that may have been involved, review bank statements, and contact your client,” noted Sircar.

After requesting to see the routing numbers used by Vista Ridge, Dapper Dashers realized the numbers were wrong. In response, Vista Ridge produced an email from December 16, 2022, from "Dapper Dashers Accounts Receivable" advising of new accounting procedures for 2023. That email explained the new account numbers to use for future payments.

Event participants had a copy of the email to review. It had few tell-tale errors! The email points to the growing sophistication of cybercrime, as it was devoid of obvious red flags such as grammatical and spelling errors, links, and attachments.

However, the audience was able to identify mistakes that should have garnered attention, including that the email was sent on a Saturday from a Gmail account, was signed by the accounts receivable department and not an individual, and contained a slightly inaccurate slogan for Dapper Dashers (Stylish Service instead of Delivering in Style).

How did the fraudster get into Dapper Dashers?

A penchant for comic books proved to be Hunter’s undoing, as he clicked on an email with a link that promised to point him to upcoming comic book conventions. Unbeknownst to Hunter, the link opened a digital door for a hacker.

“The hacker wanted information about the Dapper Dashers’ wire transactions,” said Crow. “With a few clicks they found the information and hatched a plan. Using the approaching New Year as an excuse, they sent an email claiming to be from the Dapper Dashers, asking clients to redirect next year’s payments into a fraudulent account.”

Prudent organizations would immediately determine the extent to which the hacker has infected their systems. If protected health information was stolen, there may be notification obligations.

Similarly, there may be notification obligations for regulatory and legal data that was compromised. “There might be notification obligations in various contracts, depending on the terms. It would also be advisable to check in with other clients, just to ask them about the payment information they have for your company, but don’t mention there was a breach or security incident,” Sircar explained.

Calling the FBI would be a good starting point. “Local police tend not to handle these types of things,” commented Sircar.

Though it may seem that Hunter should be fired, the attorneys questioned whether he had received adequate training. The decision would likely boil down to employee policies; a central issue would be the use of company email for personal items.

Avoid the 'B-Word'

“Coach your employees to say there was a security incident, not a breach,” advised Sircar. “Also, the information should be on a need-to-know basis, even for internal stakeholders.”

Vista Ridge may not have been the victim of a data breach, but the fact remains the company wired funds to a

fraudulent account, so it is vital to identify potential remedies for the situation in the fastest possible time frame.

“The first thing is to try and get the money back,” Fanning said. “You may want to contact the bank or the authorities. The money is traceable so it’s possible it could be retrieved, and the problem would be solved. Mayukh, in your experience, how often does this happen?”

“Rarely, if ever,” Sircar replied.

Value of Insurance

Though very few types of insurance cover these incidents, it may be worthwhile to review the policy. “These policies do exist, but they are usually troublesome and problematic,” noted Allen N. Trask III, a Ward and Smith attorney with extensive knowledge of insurance counseling, who happened to be in the audience.

A situation such as this would fall under the umbrella of employee fidelity, which deals with insider threats. “This sometimes gets wrapped up in what’s called a cybersecurity fidelity bond. Oftentimes, these policies carry heavy premiums, high deductibles, and very onerous conditions,” Trask explained.

Some of the terms required for compliance typically include holding employee training, submitting monthly scores on cyber-readiness, and record-keeping. “It may be so onerous you wonder about the utility of the coverage, though there are situations it could make sense. My advice would be to contact an agent with experience in the matter,” added Trask.

Phishing Scams and Documentation

Vista Ridge should take immediate action to determine whether it has also been the victim of a phishing scam. Reviewing internal systems, stopping other payments, interviewing employees and preserving any and all forms of documentation could be advisable courses of action.

“Inevitably, we have to figure out who bears the burden of responsibility,” noted Fanning.

Documentation is vital for providing the FBI with a timeline. Determining whether vendor payment information has been compromised is also essential, as there may be confidentiality obligations. The laws can vary across industries and borders, and there may be an obligation to report a fraudulent attack.

“Contacting an attorney would be a good idea,” commented Sircar. “The aggrieved party is going to come asking for the money, so make sure all of the information is being documented and preserved. Avoid starting the process from a position of hostility and try to be cooperative, as it will make everything go much easier.”

Of course, the situation would not have occurred if the Dapper Dashers had not been hacked. “Figuring out if they were negligent in a way that allowed the situation to occur is critical. An attorney would also review whether reasonable prevention efforts had been made and whether the company had a history of this happening,” Fanning said.

Vista Ridge is not blameless in the situation, as the company responded to modified wiring instructions with a number of red flags on a Saturday and never sought verification. “It may not be a surprise for many of you that North Carolina courts have not addressed this issue. As far as the states that have, a consistent theme is the hacked party is not always going to be the responsible party,” noted Fanning with a chuckle.

So who is the bad apple?

The courts will look at which party was in the best position to prevent the fraud. Verifying payment instructions is now an industry standard, partially due to the pervasiveness of wire fraud in real estate.

“I sent a wire to a client yesterday…I got eight emails from our accounting department…plus the bank that was going to receive it and the bank sending the wire. It’s unfortunate…this process could be so easy and fast, yet because of this fraud, it requires independent verification along the way,” Fanning commented.

To shed light on common employee justifications and mistakes, the attorneys introduced a new character, a Vista Ridge employee in accounts payable, Darcy. Her reasoning for initiating the wire was that it was not uncommon to receive wiring modifications at the end of the year, she wanted to avoid payment delays, and verifying instructions are simply not a part of the company’s standard operating procedures.

Wait, is Malware Bad?

The scenario continues by looking at the IT infrastructure that allowed the phishing email. The clues for what happened at Dapper Dashers pointed to Lawson, the son of the owners, who is also head of IT and accounting. The company had three hacks in five years. After the first one, a reminder was sent asking employees to avoid clicking on phishing emails.

Calling in a pro seemed advisable after the second incident, so Lawson reached out to the family’s ‘computer expert’ Cousin Eddie, who installed something called malware.

Once the smoke clears, companies should perform a thorough review of internal processes. Conducting additional training and addressing incidences of wire fraud/data breaches within contracts would also be advisable strategies.

A Failure to Plan Incident Response Planning

Understanding that anxiety, stress, and urgency can result in poor decision making, it is critical to have an incident response plan in place. “When something happens, being able to just go through and check all the boxes as far as who to contact, from the FBI, insurance providers, attorneys, and IT professionals, can be a big help so you’re not scrambling for the information,” advised Sircar.

A plan can be an effective means of avoiding the tendency to panic. Maintaining a clear head in a crisis is essential. “It’s also important to avoid the ‘B’ word unless it’s been confirmed by IT because a breach opens up a dearth of notification obligations,” Sircar explained.

Updating policies, payment information, and contracts is a necessity. Similarly, it’s a good idea to contact an attorney for help revising contract terms to ensure that vendors and partners train employees and have safeguards, as well as address responsibility in the event of an incident, Sircar concluded.

“Anyone who watched The Sopranos knows about the importance of closure,” laughed Crow. “With that in mind, the wire trace from Vista Ridge led to Alex, a 20-year-old college student who wanted to fund Nicholas Cage’s second efforts to steal the Declaration of Independence as a part of National Treasure’s 20-year anniversary celebration.”

That concluded the Live Action Role Play session. *No businesses, employees, college students, or famous actors were harmed in the making of this illustration.* But for issues related to a company's data security, we advise forming your response team, generating a solid response plan, training, updating your policies and procedures, and raising awareness regarding cyber-crime.

--