Who ME?

WHAT ATTORNEYS SHOULD KNOW ABOUT ONLINE FRAUD.

WRITTEN BY **MARK STACHIW**

Avoiding Cybercrime and Online Fraud in the Workplace

A recent movie, *The Beekeeper,* opens with a scene out of a horror movie. An elderly woman, who is otherwise sophisticated, is lured into an online cybersecurity scam where all of her bank accounts are cleaned out. The cybercriminal uses well-worn techniques to scam her—not asking for bank or other personal information—but acting as if trying to help her stop malware from erasing her hard drive. If you think this can only happen to the unsophisticated, that's not always the case. In a recent article in the *New Yorker,* Charlotte Cowles details how even a sophisticated reporter can be duped into handing over $50,000 to an online scammer.

The Most Common Workplace Cybercrime Scams

Attorneys representing corporations should be aware of several cybercrimes that are often being perpetrated in the business world. Knowing about these scams will also help attorneys protect their own law firms from the risks of cybercrime. The top scams typically involve wire transfer requests, vendor payment change requests, escrow-related transactions, and the use of spoofed email addresses and telephone numbers.

One of the most common scams targets employees—usually in the finance department—receiving an email allegedly from an executive instructing the wiring of money to some account for an alleged transaction. In this scenario, the executive is usually not available for confirming the wire, or the employee fails to confirm with the executive, and the wire goes out to a cybercriminal's account. Another common internet scam involves an employee receiving an email purporting to be from an existing vendor that requests a change to the bank details or where to send the vendor's payment. Yet another scam, which is especially prevalent in the real estate industry, is an email claiming to be from a seller of real estate to an escrow firm detailing where to send payment in connection with a real estate sale.

In many cybercrime scams, the perpetrator uses social engineering to get a name, email address, and other personal information and has spoofed an email address or telephone number to make emails or calls appear to be legitimate. If the cybercriminals have hacked into an email system, they may even use the real person's email to send fraudulent communications.

Recourse for Cybercrime Scams

In many cases, legal recourse may be limited. Often, cybercriminals quickly move fraudulently received money out of the account it was sent to, taking it outside the reach of the bank to claw the money back—even if the victim is aware of the crime in time to try and reverse the transaction. Moreover, financial institutions will often take the position that they were unaware of the crime and that the transfer was made by the victim. This applies to wire transfers as well as mobile app-based money transfer platforms such as Zelle. In 2023, Zelle instituted a policy that allows for recovery under specific circumstances. While insurance may help to cover losses, this assumes that a loss exceeds the deductible for the policy.

Tips for Preventing Cybercrime in the Workplace

First, educate all employees of the risk of cybercrime. Such training should include examples of typical cybercrimes, especially those that are perpetuated through phone, email, and instant messaging. Employees should not ever engage in any transaction out of the ordinary without confirming the transaction through independent means. Processes for confirming validity of requests should become standard protocol. Employees who can originate electronic financial transactions should treat each one that is out of the ordinary as requiring two-factor authentication—e.g., requiring communications with the possible payor through at least one or two different mechanisms other than the medium in which the request was made. This should include communication separately originated by the employee (not the cybercriminal). For example, calling the executive or the vendor using numbers that the employee already has for the contacts. The employee should not call the number listed in the email itself since the cybercriminal may have used a fake phone number. Additionally, employees should view with skepticism any calls purporting to be from the government, the bank, credit card companies, or even vendors. It is easy for scammers to spoof any telephone number to have it come up on caller ID as an institution such as a bank. Employees should also treat all requests for a change in who an employee may communicate with as a potential red flag. When receiving such a request, the employee should communicate with the person who they have been in regular contact with previously, via a second method to authenticate the validity of the change request.

Second, after putting training and processes in place, companies should also periodically test whether employees are following the protocol. This could consist of emails being sent that spoof existing employees asking for wire transfers and requests from vendors for changed wire instructions. The object would not be for punishment but to reinforce the training and compliance.

Third, companies should consider adding an email extension to their email server that prominently notifies the recipient when an email is from outside the company's domain. While this will not stop a cybercriminal that has hacked the company's email system, it will help deter the vast majority of email scams

that originate outside the company's email system.

What to Do After Discovering a Cybercrime Scam Occurred

Once a company finds itself the victim of cybercrime, steps should immediately be taken to try to reverse the fraudulent transaction. Depending on how quickly the cybercrime is uncovered, there may be a possibility that the transaction can be reversed or some of the money recovered.

A business that has become a victim of a cybercrime scam will want to consider whether the loss is covered by an existing insurance policy. Some business policies may cover fraud or cybercrime—even if they are not cyber insurance policies. A company that regularly engages in electronic financial transactions of significant amounts should consider buying insurance against cybercrime.

A company experiencing a loss will want to report the crime to the appropriate authorities, which in most cases will be the Federal Bureau of Investigation. Finally, the company will want to consult with its attorneys to see if there are any claims that can be brought against third party actors that may have opened the door to the fraudulent actions. For example, if a vendor's system was hacked that led to payments being redirected to the cybercriminals, the company may want to raise such breach for indemnification.

While these steps will not eliminate all possibilities that a company may become the victim of a cybercrime scam, they will help make it less likely and reduce the amount of loss if it occurs.

Key Takeaways for Preventing Cybercrime Scams in the Workplace

Businesses can help avoid becoming a victim of online fraud by implementing the following internal protocols in the workplace:

- training employees on cybercrime and the type of activity that should always be validated;
- creating processes for obtaining verifications and authentication of requests that may be suspect; and
- taking swift action to cure once a breach has been recognized. **TBJ**

This article, which was originally published on Klemchuk's Ideate *blog, has been edited and reprinted with permission.*

MARK STACHIW is of counsel to Klemchuk. He has over 30 years of corporate, securities, governance, regulatory, and transactional experience serving as the general counsel for publicly traded, and divisions of publicly traded, companies and a private equity firm.