LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Financial Regulatory Practice November 26, 2019 | Number 2566

Financial Firms Beware: Dangers Lurk in the Cloud

US regulators are calling attention to financial firms' obligations to protect against evolving cybersecurity threats.

On October 2, 2019, the Financial Industry Regulatory Authority (FINRA) issued an information notice to members warning of a growing cybersecurity threat: cloud-based email account takeovers (ATOs). These ATOs are a form of account compromise or takeover that specifically targets cloud-based email platforms.

According to FINRA, the risk of ATO attacks has escalated dramatically in the past year, particularly for financial services firms. FINRA — which did not cover ATOs in its December 2018 Report on Selected Cybersecurity Practices — 2018 — noted in the new ATO alert that several member firms have reported ATO breaches in the past six months. In the alert, FINRA provided extensive information on the methods cybercriminals use to execute ATO attacks and, importantly, how to detect, prevent, and respond to such attacks if they occur.

How ATO Attacks Work

More sophisticated than direct email scams, ATO perpetrators use phishing, impersonation, social engineering, or brute-forcing techniques to obtain log-in credentials to access a victim's cloud-based email account. Cybercriminals then shadow the email account for weeks or months in an attempt to steal and monetize confidential information, or discover opportunities to misdirect money transfers by tricking unsuspecting colleagues or clients into sending funds to external bank accounts under the attacker's control. The attacker will often tamper with a victim's email account to prevent the victim from discovering the fraudulent directives and transactions. If a cybercriminal is able to compromise the account of an employee with administrative IT privileges, the criminal may use the account as a platform to launch a larger-scale attack.

Preventing and Responding to ATO Attacks

FINRA's notice includes a list of practices that FINRA has observed firms implement in order to both prevent ATOs and respond to ATOs after they have occurred. The notice observes that two-factor authentication (2FA) for external email access is critical for preventing ATOs. Rather than rely on a single password, 2FA requires an additional layer of protection such as a PIN, a temporary security token, or biometric identification. While not a guarantee, 2FA can limit an attacker's ability to access an email account even if they are able to obtain the account password. FINRA noted that most cases of system infiltration occurred at firms that had not implemented 2FA.

Other preventive measures FINRA emphasized include:

- Archiving email externally from the main email server to retain a full record of inbound and outbound mail, regardless of inbox tampering
- Monitoring for suspicious log-in attempts and maintaining robust account access logs for an adequate period of time
- Exercising close control of administrator account access and privileges

Victims of successful ATO attacks should take all necessary steps to contain, analyze, and prevent residual or ongoing damage, especially if illicit access was obtained for administrator-level accounts. Firms should also determine if any clients' personal or corporate information was compromised, and if so, make the appropriate disclosures to regulators and law enforcement authorities. Firms should continually assess the strength of their cybersecurity controls and regularly monitor customer accounts for any indications that customer account security has been compromised. Firms should also strongly consider working with experienced legal counsel, who may also retain independent outside forensic experts, in order to document root causes, review the reasonableness of the response measures, assess damage, and, most importantly, develop a documented plan of remediation and correction. This step may be essential in persuading government investigators or auditors that a mature (compliant) information security program is — or soon will be — in place.

NFA Cybersecurity Guidance Aligns With FINRA's Concerns

In early 2019, the National Futures Association (NFA) amended its 2016 Interpretive Notice entitled NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Interpretive Notice). The NFA Interpretive Notice requires all NFA members (including US and non-US members) to enact a written information systems security program (ISSP) as an effective guide to navigating potential or actual threats to their information technology systems. The ISSP standards, procedures, practices, and adopted safeguards must be designed and implemented by each firm in a way that is reasonably appropriate for their individual business circumstances, including the firm's "size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities."

The Interpretive Notice and accompanying Cybersecurity FAQs do not establish specific technology or format requirements, but do require firms to:

- Document and implement procedures reasonably designed to prevent and detect potential cybersecurity threats
- Assess risks posed by third-party services that may have access to the firm's systems
- Identify the specific topics, appropriate to the security risks the firm faces, that are covered in the firm's cybersecurity training program
- Obtain written approval for the ISSP by the firm's Chief Executive Officer, Chief Technology Officer, or "senior level officer with primary responsibility for information security or other senior official who is a listed principal and has the authority to supervise the Member's execution of its ISSP"
- Create a training program and provide training to employees upon hiring and at least annually thereafter during their employment, but more frequently if warranted
- Create an incident response plan that addresses how a firm will manage cybersecurity breaches, communicate with both internal and external parties in the event of an attack, and restore compromised systems and data

- Notify the NFA (and other relevant regulators and law enforcement agencies) of cybersecurity incidents related to their business in an appropriate manner and timeframe
- Monitor and review the efficacy of the ISSP at least once annually, and review the effectiveness of the cybersecurity controls in place
- Update the ISSP and upgrade cybersecurity defenses as needed
- Maintain appropriate records of all documentation relating to ISSP adoption, implementation, and cybersecurity compliance

The NFA Interpretive Notice is aligned with current and previous FINRA guidance on cybersecurity. Like the NFA, FINRA emphasizes the importance of a sound governance framework for cybersecurity; written supervisory procedures; senior management engagement; internal and external risk assessment; strong technical controls to protect confidential information and critical systems; incident detection and response; breach containment and recovery; employee and client communication; and training and awareness appropriate to a firm's business and operations.

CFTC Case Study: What Not to Do When You Are the Victim of an ATO Attack

Although not arising in the context of cloud-based accounts, a September 12, 2019, enforcement action by the US Commodity Futures Trading Commission (CFTC) underscores the email dangers described by FINRA. In the CFTC matter, the Commission issued an order and notice of settlement for a cybersecurity breach that compromised the email system of a futures commission merchant (FCM) in Chicago, which resulted in compromised client data and a theft of US$1 million of client funds.

In the order, the CFTC finds that on February 28, 2018, an IT engineer at the FCM was baited with a phishing email from a hacked financial security organization account, and unwittingly provided administrator-level log-in credentials to the firm's email systems. The cybercriminals then used the credentials to access the administrator's account, and from there, accessed other employee accounts and the confidential client information contained therein. Despite noticing irregularities, the IT engineer did not fully realize that the account had been compromised until two days later. The IT engineer then notified the firm's management, who instructed the engineer to direct all employees to reset their email passwords, but did not consult the firm's ISSP for guidance.

That same day, the hackers used information they had accessed in various email accounts on the FCM's system to impersonate a client and direct the firm to wire US$1 million to a bank account in Hong Kong. Rather than verify the wire transfer request via an independent channel (*e.g.*, a phone call to the client), the customer service specialist who received the email responded to the email request directly to confirm that the "client" did in fact want the funds transferred. Despite various levels of supervision and approval backstops within the firm's finance department, the wire transfer was executed as requested that day. The next business day, the actual client contacted the FCM to inquire why US$1 million had been wired out of the client's account. Only then did the firm realize the extent of the system breach it had suffered.

The CFTC held the FCM accountable for the breach and loss of funds and confidential client information under CFTC rules, faulting the firm for failures that "allowed" cybercriminals to perpetrate the theft. Specifically, the CFTC found that the firm breached its duty of diligent supervision under Regulation 166.3 and failed to meet the customer records and information safeguarding obligations under Regulation 160.30. According to the order, after the attack the firm's employees did not consult or follow its ISSP, which the CFTC further criticized for not being "reasonably tailored" to the firm's operations. The CFTC also found that the firm's chief compliance officer, who was responsible for its ISSP, was not familiar enough with IT or cybersecurity "to adequately evaluate the sufficiency of [its] cybersecurity policies and trainings."

The CFTC also stated that although the defrauded client was immediately reimbursed for the diverted funds, the FCM did not investigate the impact of the breach on broader client information until several weeks later. The co-CEOs of the firm also decided not to inform other clients of the system breach, and in fact endeavoured to conceal the breach from its wider client base and the general public due to the reputational damage they presumably anticipated. The firm notified its clients of the breach almost a year later, after the CFTC began its investigation of the matter. Importantly, the CFTC noted that pursuant to Regulation 1.55(i), timely disclosure of system breaches to existing and prospective clients may be critical, as the information may be "material to the customer's decision to entrust … funds to and otherwise do business with" the firm.

For these failures, the CFTC ordered the FCM to pay US$1 million in restitution to the defrauded client (which the firm had already done, and so was credited by the CFTC) and to pay a US$500,000 civil penalty. The CFTC also ordered the firm to take remedial steps to improve its cybersecurity systems, procedures, and supervision, and to submit a final report of its remedial actions within three months of the order.

Preventing and Mitigating Business Email Compromise

As compared with other cyber threats — such as nation-state espionage or advanced criminal enterprises stealing large databases — the risk of a business email compromise event is comparatively manageable to mitigate in basic ways. The FBI's advice is straightforward, long-standing, and therefore potentially viewed as a quasi-standard of care for regulated financial entities. According to the FBI, employees must be specifically trained to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information
- Ensure the URL in emails is associated with the business it claims to be from
- Be alert to hyperlinks that may contain misspellings of the actual domain name
- Refrain from supplying log-in credentials or personally identifiable information in response to any emails
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits
- Keep all software patches on and all systems updated
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring that the sender's email address appears to match the person the email is coming from
- Ensure the settings on employees' computers are enabled to allow full email extensions to be viewed

Most companies do some form of anti-phishing training, but not all training programs are equivalent. Senior management will want to verify that their IT team is appropriately using anti-phishing security awareness programs such that successful phishing attempts are drastically reduced.

Finally, if funds are misdirected in response to a scam notwithstanding preventive measures, time is of the essence. Business email compromise scenarios should be fully integrated into incident response plans. Law enforcement and financial institutions can take meaningful, effective steps to reverse fraudulent wires if they catch the error quickly. Even an hour's delay in reporting can mean the difference between sustaining a complete loss or recovering the funds.

Conclusion

The FBI statistics on email compromise events are staggering in terms of the number of events, the simplicity of the steps required to avoid the scams, and the total dollars lost.[1] Latham & Watkins has advised clients on dozens of such business email compromise events in the past two years alone, and the tide shows no sign of receding. FINRA's new guidance, along with the NFA's Interpretive Notice and the CFTC's recent enforcement action, serve as timely reminders of the importance of robust governance and cybersecurity measures.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

William R. Baker III
william.baker@lw.com
+1.202.637.1007
Washington, D.C.

John J. Sikora Jr.
john.sikora@lw.com
+1.312.876.6580
Chicago

Serrin Turner
serrin.turner@lw.com
+1.212.906.1330
New York

Yvette D. Valdez
yvette.valdez@lw.com
+1.212.906.1797
New York

Stephen P. Wink
stephen.wink@lw.com
+1.212.906.1229
New York

Douglas K. Yatter
douglas.yatter@lw.com
+1.212.906.1211
New York

Deric Behar
Knowledge Management Lawyer
deric.behar@lw.com
+1.212.906.4534
New York

You Might Also Be Interested In

FINRA Publishes Its 2019 Report on Examination Findings and Observations

FSB Concerns Over Cloud Concentration in Financial Services Continues

The Systemic Importance of Cloud-Based Service Providers to Banks

Report on IT Failures in the UK Financial Services Sector

Endnotes

[1] *See* FBI Public Service Announcement, Business Email Compromise: The $26 Billion Scam (September 2019).