CADWALADER

Cadwalader, Wickersham & Taft LLP
www.cadwalader.com

Clients&FriendsMemo

Law Firm Data Breaches Demonstrate the Expanding Scope of Cyber Attacks

January 17, 2017

In a case of "cyber meets securities fraud," the United States Attorney's Office for the Southern District of New York ("SDNY") recently indicted three foreign nationals on charges of insider trading, wire fraud, and computer hacking for allegedly trading on information they stole from the computer networks of two major New York law firms.[1] A parallel enforcement action brought by the Securities and Exchange Commission – its first time bringing civil charges based on the hacking of a law firm's computer network – alleges insider trading and other violations of the Securities Exchange Act of 1934.[2] The case is a wake-up call that hackers are becoming more creative both in their choice of victims and in how they use the information they steal, requiring companies to reconsider what type of data is prone to hacking and whether their security protocols are sufficient to detect and prevent it. It is also a reminder to certain federal and state regulated entities that they may soon have to comply with new cybersecurity rules requiring robust policies and procedures governing how confidential data and computer networks are handled and protected.

Hacking Schemes Are Becoming More Creative

The criminal defendants – Iat Hong, Bo Zheng, and Chin Hung – live in Macau and mainland China and are alleged to have attacked the computer networks of multiple law firms to identify and steal confidential client information. In each case in which they were successful, it is believed the defendants used a combination of malware and stolen login credentials to gain access to the firms' networks. Using that access, the defendants allegedly stole emails containing information about potential client merger and acquisition activity, and then traded in the securities of those companies, earning over $3 million in illicit profits.[3]

---

1 *See* Indictment, *United States v. Iat Hong*, et al., S1 16 Cr. 360 (Oct. 13, 2016), *available at* https://www.justice.gov/usao-sdny/press-release/file/921006/download.

2 *See* Complaint, *SEC v. Iat Hong,* et al., 16 Civ. 9947 (Dec. 27, 2016), *available at* https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf.

3 Further demonstrating how hacking groups are increasingly targeting a wide array of victims for a variety of different purposes, the Indictment alleges that the defendants also hacked into the networks of robotics technology companies in the United States and Taiwan to steal confidential technological data.

Another recent case further illustrates this trend. In late 2015, prosecutors in the SDNY charged three individuals with engaging in multiple computer-based crimes, including a massive scheme to steal over 100 million customer records from several financial institutions.[4] In that case, the defendants did not steal customer records to simply withdraw money from the customers' bank accounts or run up charges on their credit cards. Instead, they allegedly used the stolen customer information – including email addresses and telephone numbers – to market securities to the customers as part of a sophisticated pump-and-dump securities fraud scheme. As the United States Attorney for the SDNY stated when the charges were announced, "[t]he charged crimes showcase a brave new world of hacking for profit. It is no longer hacking merely for a quick payout, but hacking to support a diversified criminal conglomerate."

Anyone Can Be a Target

These cases demonstrate the ever-expanding scope of cybercrime, both in terms of the victims whose computer networks are targeted and the methods by which hackers exploit the information they steal.

With respect to potential victims, these cases show that hackers are thinking creatively about where they might find valuable confidential information – whether that information is a proposed merger or a business's trade secrets – and are looking both to corporations and their third party vendors as potential targets. Certain vendors, such as payment processors, professional services firms, and medical billing companies, are tempting targets because they often retain valuable individual and company information. Even vendors that do not retain confidential customer information may be indirect targets for hackers. For example, if a vendor has privileged access to a client's internal network, hackers could effectively use that access as a "back door" to compromise the clients' systems.[5]

Regulators are aware of the potential cybersecurity risks presented by third party vendors and are starting to implement new rules to address them. For example, in October 2016, three federal banking regulators – the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation – announced potential new cybersecurity standards for

---

[4] *See* Press Release, "Attorney General and Manhattan U.S. Attorney Announce Charges Stemming from Massive Network Intrusions at U.S. Financial Institutions, U.S. Brokerage Firms, Major News Publications and Other Companies" (Nov. 10, 2015), *available at* https://www.justice.gov/opa/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network.

[5] It is reported that the hackers responsible for a 2013 data breach of a major retailer, which resulted in the theft of millions of customer credit and debit card records, gained access to the network by first compromising the system of a third party vendor that provided heating and air-conditioning services to the retailer's stores. *See* "Heat Systems Called Door to Target for Hackers," *The New York Times* (Feb. 4, 2014), *available at* https://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html?_r=0.

large financial institutions.[6] Among other things, the rules would require the adoption of robust compliance programs to evaluate and manage the cybersecurity risks posed by "external dependencies" such as third party vendors. Similarly, the New York Department of Financial Services ("DFS") recently issued new cybersecurity rules that require regulated banks, insurance companies, and other financial institutions to adopt written policies and procedures designed to ensure the security of confidential information held by third party vendors.[7] Among other things, the DFS rules require regulated institutions to evaluate the risks posed by their third party vendors, conduct due diligence on vendors' cybersecurity programs, and mandate minimum cybersecurity practices to be adopted by the vendors. The new DFS rules go into effect on March 1, 2017.[8]

Conclusion

As more confidential information is stored electronically and as more business activity is transacted exclusively on the Internet, economically motivated cybercriminals will find new targets for hacking and creative ways to steal valuable data and defraud individuals, corporations, and the public. These recent prosecutions are departures from typical schemes in which cybercriminals use stolen information to make a quick profit through straightforward identity theft or credit card fraud. Instead, they reflect a trend of increasingly sophisticated hackers who are thinking carefully about both the types of data that are available for theft and the means by which that data could be exploited to maximize its profit-generating potential. These cases are a reminder that anyone in possession of sensitive customer or company data should remain vigilant and take reasonable and appropriate steps to protect their systems from attack.

* * * *

If you have any questions, please feel free to contact any of the following Cadwalader attorneys.

Joseph Moreno	+1 202 862 2262	joseph.moreno@cwt.com
Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com

---

6 *See* Joint Press Release, "Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards" (Oct. 19, 2016), *available at* https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm.

7 *See* Press Release, "DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions" (Dec. 28, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1612281.htm. The updated rules are subject to a 30-day notice and comment period, and may therefore be revised before they go into effect.

8 *See* Cadwalader Clients & Friends Memo, "New York State Revises 'First-In-Nation' Cybersecurity Rules" (Jan. 10, 2017), *available at* http://www.cadwalader.com/resources/clients-friends-memos/new-york-state-revises-first-in-nation-cybersecurity-rules.