KIRKLAND **ALERT**

March 19, 2018

Insider Trading Charges Levied in Connection with Data Breach

On March 14, 2018, a former Equifax executive was civilly and criminally charged by the U.S. Securities and Exchange Commission and the U.S. Department of Justice for allegedly exercising stock options and selling Equifax stock after learning about Equifax's data breach in 2017. This represents the first time that the SEC or DOJ has charged a corporate executive, whether civilly or criminally, in connection with a data breach. Further, the SEC and DOJ litigation comes on the heels of the SEC's recent cybersecurity guidance, which discussed insider trading following a data breach. Accordingly, companies should consider closely reviewing their insider trading and incident response policies for potential enhancements.

The case represents the first time that the SEC or DOJ has charged a corporate executive, in his or her individual capacity, whether civilly or criminally, in connection with a data breach.

The Alleged Insider Trading

According to the SEC and DOJ, Equifax learned of a potential data breach in late July 2017. Those working on the breach response were told to keep the breach confidential and were subjected to a special trading blackout period, per Equifax's insider trading policy. Equifax also established a team that worked on preparing the infrastructure to notify consumers who were potentially affected by the breach. Known as Project Sparta, this team was told that an "unnamed client" experienced a large data breach, not that Equifax was the entity that was breached.

During the afternoon of Friday, August 25, 2017, the SEC and DOJ allege that Jun Ying, the former Chief Information Officer ("CIO") of Equifax's U.S. Information Systems, received emails regarding Project Sparta. By that evening, Ying allegedly deduced that Equifax was the company that was breached. On Monday morning, Ying searched the Internet for information about the impact of Experian's 2015 data breach on Experian's stock price. Shortly thereafter, Ying allegedly exercised all of his vested options to buy Equifax shares, and subsequently sold those shares. In the process, he allegedly collected more than $950,000 and avoided more than $117,000 in losses that he would have suffered if he sold after Equifax's public disclosure of the data breach on September 7. Equifax conducted an internal investigation into Ying's trading and terminated his employment on October 16, 2017.

Key Takeaways

The SEC and DOJ litigation against Jun Ying is notable for several reasons:

- The case represents the first time that the SEC or DOJ has charged a corporate executive, in his or her individual capacity, whether civilly or criminally, in connection with a data breach.

- Data breaches are not technical problems that are solely the province of the IT department. Instead, coordination between IT, legal, executive management and the board is necessary to ensure compliance with federal securities laws in the wake of a data breach.
- Companies should consider closely reviewing their insider trading and incident response policies for potential enhancements, particularly with respect to trading blackout periods.
- The risk of insider trading following data breaches might be higher than previously thought, as a recent study suggests that some companies have experienced greater stock price fluctuation after recent data breaches than those in prior years.
- The SEC is likely to place greater scrutiny on suspicious trading around data breaches.
- The SEC's recent cybersecurity guidance, which addressed insider trading following the discovery of a data breach, appears to be targeted in part at alleged conduct like Ying's. It is possible the SEC might be planning enforcement actions relating to other issues mentioned in the guidance, such as adequate and timely public disclosures related to data breaches.

Companies should consider closely reviewing their insider trading and incident response policies for potential enhancements, particularly with respect to trading blackout periods.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Lauren O. Casazza, P.C.
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/lcasazza
+1 212 446 4661

Norm Champ, P.C.
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/nchamp
+1 212 446 4966

Gianni Cutri, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/gcutri
+1 312 862 3372

Asheesh Goel, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/agoel
+1 312 862 3005

Brian P. Kavanaugh
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/bkavanaugh
+1 312 862 2015

Joshua N. Korff, P.C.
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/jkorff
+1 212 446 4943

Sunil Shenoi
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/sshenoi
+1 312 862 3028

Erica Williams, P.C.
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/ewilliams
+1 202 879 5044

Seth Traxler, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/straxler
+1 312 862 2241