UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **v.** **JUN YING,** **Defendant.**	**Case No.** **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff, Securities and Exchange Commission (the "Commission"), files its complaint and alleges that:

SUMMARY

1. Defendant Jun Ying ("Ying") committed securities fraud by engaging in illegal insider trading. After being entrusted with material, nonpublic information about a massive cyber-intrusion and data breach suffered by his employer, Equifax Inc. ("Equifax" or "the company"), Ying exercised all his vested Equifax stock options and sold the shares prior to the public announcement of the breach. By selling when he did, Ying avoided losses in excess of $117,000.

2. By the conduct detailed in this Complaint, Ying violated Section 17(a) of the Securities Act of 1933 ("Securities Act") [15 U.S.C. § 77q(a)], Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") [15 U.S.C. § 78j(b)] and Rule 10b-5 [17 C.F.R. § 240.10b-5] thereunder. Unless enjoined, Ying is likely to commit such violations again in the future.

3. The Commission seeks a judgment from the Court: (a) enjoining Ying from engaging in future violations of the antifraud provisions of the federal securities laws; (b) ordering Ying to disgorge an amount equal to the losses avoided as a result of the actions described herein, with prejudgment interest; (c) ordering Ying to pay a civil monetary penalty pursuant to Section 21A of the Exchange Act [15 U.S.C. § 78u-1]; and (d) prohibiting Ying from serving as an officer or director of a public company.

JURISDICTION AND VENUE

4. The Commission brings this action pursuant to Sections 20(b) and 20(d) of the Securities Act [15 U.S.C. §§ 77t(b) and 77t(d)] and Section 21(d) the Exchange Act [15 U.S.C. § 78u(d)].

5. The Court has jurisdiction over this action pursuant to Sections 20(b), 20(d) and 22(a) of the Securities Act [15 U.S.C. §§ 77t(b), 77t(d), and 77v(a)], and

Sections 21(d), 21(e), 21A and 27 of the Exchange Act [15 U.S.C. §§ 78u(d), 78u(e), 78u-1, and 78aa].

6. Ying, directly or indirectly, used the means or instruments of interstate commerce, the mails, or the facilities of a national securities exchange in connection with the acts described herein.

7. Venue is proper under Section 22 of the Securities Act [15 U.S.C. § 77v], Section 27 of the Exchange Act [15 U.S.C. § 78aa] and 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims made herein occurred in the Northern District of Georgia. In addition, Ying currently resides in the Northern District of Georgia.

DEFENDANT

8. **Jun Ying**, age 42, is a resident of Atlanta, Georgia. He was an employee of Equifax Inc. from January 2013 until October 2017, and was the Chief Information Officer ("CIO") of Equifax's United States Information Systems ("USIS") business unit at the time of his departure. At the time of the Equifax breach, Ying was a leading candidate to succeed the then-current global CIO of Equifax, and was, in fact, offered the job on September 15, 2017. As CIO of USIS, Ying was often entrusted with nonpublic information about Equifax.

OTHER RELEVANT ENTITY

9. **Equifax Inc.**, an information solutions and human resources company, is a Georgia corporation headquartered in Atlanta, Georgia. Equifax's common stock trades on the New York Stock Exchange under the symbol "EFX." Equifax is one of three major consumer credit bureaus that collect and maintain a vast amount of consumer credit information for the purpose of offering credit and demographic data and services.

STATEMENT OF FACTS

I. THE EQUIFAX CYBERSECURITY BREACH.

10. On July 29, 2017, Equifax's security department observed suspicious network traffic associated with the company's consumer dispute portal, which is a part of Equifax's website where consumers dispute items on their credit reports.

11. In response, the security department immediately blocked the suspicious traffic and continued to monitor the network. The next day, after observing additional suspicious activity, the security department took the portal offline.

12. On August 2, 2017, Equifax retained the cybersecurity group at an Atlanta law firm to investigate the incident and provide legal and regulatory advice. That same day, Equifax, through the law firm, engaged an independent cybersecurity forensic consulting firm.

13. Over the next several weeks, the cybersecurity forensic consulting firm and Equifax's internal security department analyzed forensic data to determine the nature and scope of the suspicious activity. It was determined that Equifax had been subject to cyber-intrusions that resulted in a breach of Equifax's information technology ("IT") systems.

14. In accordance with Equifax's internal policies, the company classified the breach as a "critical incident" and formed a crisis action team, comprised of security, legal, and IT personnel.

15. The company designated the response to the breach as "Project Sierra," and instructed those working on Project Sierra that information related to the project was confidential and should not be shared with anyone outside of Equifax's crisis action team.

16. The forensic investigators determined that, in connection with the breach, it was likely that sensitive data, including consumers' personally identifiable information ("PII"), had been stolen. Equifax then instituted a special trading blackout period for those working on Project Sierra. Trading blackout periods are typically implemented pursuant to a company's insider trading policy to prevent trading by insiders when significant events or changes are taking place within the company.

17. As part of its response to the breach, Equifax also deployed additional security measures to protect the company's network. For example, between August 12 and 15, 2017, Project Sierra team members changed administrative credentials for hundreds of internal databases. The so-called "password reset" required the assistance of a broader group of Equifax IT employees who were not informed of the breach.

18. Equifax also established a notification and remediation plan for the millions of consumers affected by the breach. This effort, which the company designated "Project Sparta," involved setting up a website for consumers to determine whether they were affected by the breach, developing a suite of protective tools for consumers, and staffing call centers.

19. Project Sparta was kept separate from Project Sierra to limit the number of people who knew that Equifax itself had been breached. Those Equifax employees who were only part of Project Sparta were not told that Equifax had been breached, but were instead told that they were working for an unnamed client that had experienced a large data breach.

20. The company decided to handle much of the work for Project Sparta through its own Global Consumer Solutions business unit ("GCS"), which developed and

sold various personal security and identity theft defense products and services to clients.

21. On August 23, 2017, one of Ying's peers, the CIO of another Equifax business unit, was informed of the breach. He was also asked to lead the notification and remediation efforts that composed Project Sparta.

22. Ying was not informed of Project Sierra or Project Sparta at that time, nor was he made aware of his colleague's appointment to lead the soon-to-be implemented notification and remediation efforts.

II. YING IS ENTRUSTED WITH INFORMATION ABOUT THE BREACH.

23. At 2:22 p.m. on Friday, August 25, 2017, as part of Project Sparta, an email was sent to several Equifax IT personnel who were responsible for the systems that would handle the breach remediation efforts, as well as the CIOs of certain business units. Ying was among the CIOs included.

24. The email stated that GCS was working on a "**VERY** large breach opportunity" that required a dramatic increase in the capacity of the relevant technology systems, and that this was "an extremely time sensitive request," with a deadline of August 29, 2017.

25. Ying initially instructed his direct reports not to work on the project until they received additional information.

26. At 4:33 p.m. that afternoon, Ying (among other IT personnel, including several of his direct reports) received a calendar appointment invitation for a conference call at 4:45 p.m. with the subject, "URGENT / MANDATORY MEETING – Breach Opportunity." The invitation stated that Equifax's global CIO for all company operations, who was Ying's immediate supervisor, wanted the group to get "onboard on this ASAP," and that participants should prepare the IT applications under their care to handle approximately 10 million customers.

27. Ying did not initially participate in the conference call, but an IT employee who reported directly to Ying was on the call. During the call, Ying and his direct report exchanged text messages in which the direct report informed Ying that Ying's team would have to cancel their Friday evening plans to respond to the Project Sparta requests.

28. Ying then joined the conference call, and initially resisted the requests for assistance. He also expressed concern that the deadline was unrealistic. In response, the leader of Project Sparta instructed Ying to call the global CIO with his concerns.

III. YING CONCLUDES THAT EQUIFAX WAS THE REAL VICTIM OF THE BREACH.

29. At 5:26 p.m., Ying called the global CIO. The call lasted only one minute.

30. During the call, the global CIO told Ying that Ying was expected to comply with the requests. The global CIO also told Ying that, at that time, Ying did not need to know why he had to comply, but that at some point, Ying would understand what was happening.

31. At 5:27 p.m., Ying texted the direct report he had communicated with earlier, writing: "On the phone with [global CIO]. Sounds bad. We may be the one breached. . . . Starting to put 2 and 2 together."

32. After that call, Ying's demeanor towards the requests for assistance changed. Just three minutes later, at 5:30 p.m., the Project Sparta leader texted Ying to ask whether Ying had any questions after speaking to the global CIO. Ying responded, "No question right now. Actually, I don't want to know ;) I told the team to [rally]." Ying's team began responding to the requests for assistance.

33. Numerous additional communications the evening of August 25, 2017, informed Ying that this breach was unusual, and indicate that Ying used the information entrusted to him as an Equifax employee to conclude that Equifax was the victim of the breach, and that the "breach opportunity" idea suggesting a client was the victim was merely a cover story.

34. At 5:34 p.m., Ying called Equifax's global CIO again, and the two discussed the fact that the breach response plan, which called for offering credit bureau

reports from all three credit bureaus to 50 million consumers, would be highly unusual and would strain the company's resources.

35. At 5:50 p.m., Ying exchanged text messages with the same direct report he had texted with earlier that afternoon. In the texts, both men expressed that the breach situation was "crazy," and Ying stated that the company had "some crisis scenarios like this," referencing Equifax's Crisis Management Plan, which, among other things, provided a plan for responding to a breach of Equifax's systems.

36. In fact, as part of the company's training in support of the Crisis Management Plan, Ying previously had participated in a simulated crisis scenario in which Equifax's CIO was unavailable following a cybersecurity breach, and Ying was asked to step into the role of CIO for purposes of formulating a response.

37. At 6:19 p.m., another IT employee who reported to Ying emailed Ying regarding a series of meetings (unrelated to the breach) that were scheduled for the week of August 28, 2017, and were to take place in different states. These meetings were to include executives from Equifax's IT, Legal, and Security departments, as well as their counterparts at certain major retailers, and related to the business relationships between Equifax and the retailers.

38. The IT employee informed Ying that a number of senior leadership members, including the global CIO and the leader of Project Sparta, as well as

Equifax's Chief Security Officer ("CSO"), Chief Legal Officer, and VP of Cybersecurity, were cancelling their travel plans.

39. Ying confirmed the cancellations, and, in his reply emails, stated "I think you now know why." He also stated that he thought the travel cancellations were "related to all the mad scrambling . . . ."

40. At 8:55 p.m., yet another IT employee who reported to Ying forwarded Ying emails from Equifax's Senior Director of Crisis Management asking for log files for a specific database. The employee told Ying that he had concerns about producing the files to security and was unsure whether this related to the breach opportunity that was discussed on the earlier conference call.

41. At 8;59 p.m., Ying responded: "Yup. Cooperate." At this point, the securities market had been closed for several hours, and would not reopen until Monday morning, August 28, 2017.

42. At approximately 10:00 a.m. on Monday, August 28, 2017, Ying used a search engine to find information on the internet concerning the September 2015 cybersecurity breach of Experian, another one of the three major credit bureaus, and the impact that breach had on Experian's stock price. The search terms used by Ying were: (1) "Experian breach"; (2) "Experian stock price 9/15/2015"; and (3) "Experian breach 2015."

43. These searches yielded results revealing that, although the breach at Experian was much smaller than the one that Equifax faced, the public announcement of Experian's breach negatively impacted that company's stock price. Ying's internet browsing history indicates that Ying reviewed market data showing that Experian's stock price dropped approximately four percent after the public announcement of the breach.

44. By no later than 10:00 a.m. on August 28, 2017, based on nonpublic information entrusted to him by his employer, Equifax, Ying had concluded that Equifax itself was the victim of a major cybersecurity breach, despite the statements made as part of Project Sparta asserting that it was a business opportunity for an unnamed client.

45. Ying owed a duty of trust and confidence to Equifax and its shareholders not to trade on the basis of material nonpublic information that he learned through his employment with Equifax, and was aware of his duty.

46. Ying knew or was reckless in not knowing that the information that Equifax was the victim of a major cybersecurity breach was material.

47. Ying knew or was reckless in not knowing that the information that Equifax was the victim of a major cybersecurity breach was nonpublic.

IV. YING'S TRADING IN EQUIFAX SECURITIES.

48. Ying received a portion of his compensation through stock option grants and restricted shares. While Ying had exercised some of his options previously, as of October 1, 2016, Ying held 6,815 vested options, which he continued to hold until August 28, 2017.

49. Within an hour of running the internet searches regarding the September 2015 cybersecurity breach of Experian, Ying accessed his company-sponsored stock plan account with UBS Financial Services, Inc., exercised all of his vested options to buy Equifax shares, and then immediately sold those Equifax shares for total proceeds of more than $950,000.

50. These securities transactions were made on the basis of material nonpublic information and breached the duty of trust and confidence that Ying owed to Equifax and its shareholders. Ying knew or was reckless in not knowing that the information that Equifax itself was the victim of a major cybersecurity breach was material and nonpublic, and Ying used that information when making these securities transactions.

51. By selling Equifax shares before its cybersecurity breach was publicly disclosed, Ying avoided more than $117,000 in losses that he would have suffered had he not sold until after the news of the breach became public.

52. Ying's trading on the basis of material nonpublic information entrusted to him by Equifax was deceptive and fraudulent.

V. YING IS OFFICIALLY NOTIFIED OF THE EQUIFAX BREACH.

53. On August 29, 2017, the day after exercising his options and selling Equifax shares, Ying was traveling for business when he was unexpectedly called back to Atlanta by Equifax's global CIO. The global CIO did not tell Ying why he needed him to return.

54. Shortly after receiving instructions to return to Atlanta, Ying sent a text message to a work colleague at Equifax. Among other things, Ying's text told the colleague that he thought there was going to be "some big media announcement" about Equifax, that "it might be bad," and that it was why "everyone was cancelling trips this week and even next."

55. On August 30, 2017, Ying was back in Atlanta. The global CIO for Equifax officially told Ying that Equifax was the entity that had been breached. Ying then met with one of the attorneys engaged by Equifax, who confirmed for Ying what the global CIO had said, and gave him a set of instructions and directions that had been developed for that situation, *i.e.*, when an Equifax employee was told that Equifax was the entity that had been breached. After receiving the instructions and directions, such employees then became part of the Project Sierra team.

56. Unaware that Ying had already traded, the attorney told Ying that the news about the breach was confidential, should not be shared with anyone, and that Ying should not trade in Equifax securities. Ying did not volunteer the fact that he had exercised and sold all of his vested Equifax options two days before.

VI. EQUIFAX TELLS THE PUBLIC ABOUT THE BREACH.

57. After the close of the market on September 7, 2017, Equifax issued a press release and filed a Form 8-K with the Commission, announcing the cybersecurity breach and revealing that it potentially impacted approximately 143 million consumers in the United States.

58. The breach was one of the leading news stories over the next several days and was described as "one of the worst [data breaches] ever, by its reach and by the kind of information exposed to the public."

59. On September 8, the price of Equifax common stock closed at $123.23, a drop of $19.49 (nearly 14%) per share from the prior day's closing price of $142.72. Trading volume that day also increased dramatically to nearly seventeen million shares, more than a thirty-fold increase from the previous day's volume of approximately 518,000 shares.

60. On September 15, 2017, following the resignation of the then-current global CIO, Ying was offered the position of global CIO of Equifax. The offer was

subsequently withdrawn, however, after Equifax senior executives learned of Ying's trading.

61. On October 16, 2017, following an internal Equifax investigation into Ying's trading, the company concluded that he had violated the company's insider trading policy and that his employment should be terminated. At that time, Ying agreed to resign.

COUNT I – INSIDER TRADING IN CONNECTION WITH THE PURCHASE OR SALE OF SECURITIES

Violations of Section 10(b) of the Exchange Act and Rule 10b-5 Thereunder [15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5]

62. The Commission realleges and reincorporates paragraphs 1 through 61 as if fully set forth herein.

63. Ying, with scienter, by use of the means or instrumentalities of interstate commerce or of the mails, in connection with the purchase or sale of securities: (a) employed devices, schemes, or artifices to defraud; (b) made untrue statements of material fact or omissions to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices or courses of business which operated or would operate as a fraud or deceit.

64. By reason of the actions alleged herein, Ying violated Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5].

COUNT II – INSIDER TRADING IN THE OFFER OR SALE OF SECURITIES

Violations of Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)(1)]

65. The Commission realleges and reincorporates paragraphs 1 through 61 as if fully set forth herein.

66. Ying, with scienter, by use of the means or instrumentalities of interstate commerce or of the mails, in the offer or sale of securities: (a) employed devices, schemes or artifices to defraud; (b) obtained money or property by means of untrue statements of material fact or omissions to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices or courses of business which operated or would operate as a fraud or deceit upon the purchasers of the securities offered and sold by Ying.

67. By reason of the actions alleged herein, Ying violated Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

PRAYER FOR RELIEF

WHEREFORE, the Commission respectfully requests that the Court enter a judgment:

(i) finding that Ying violated the antifraud provisions of the federal securities laws as alleged herein;

(ii) permanently enjoining Ying from violating Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)], Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5];

(iii) ordering Ying to disgorge an amount equal to the losses avoided as a result of the actions alleged herein and to pay prejudgment interest thereon;

(iv) ordering Ying to pay a civil monetary penalty pursuant to Section 21A of the Exchange Act [15 U.S.C. § 78u-1];

(v) issuing an order, pursuant to Section 20(e) of the Securities Act [15 U.S.C. § 77t(e)] and Section 21(d)(2) of the Exchange Act [15 U.S.C. § 78u(d)], prohibiting Ying from serving as an officer or director of a public company; and

(vi) granting such other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, the Commission demands trial by jury in this action of all issues so triable.

Dated this 14th day of March, 2018.

Respectfully submitted,

/s/ *W. Shawn Murnahan*
W. Shawn Murnahan
Senior Trial Counsel
Georgia Bar No. 529940
Tel: (404) 842-7669
Email: murnahanw@sec.gov

M. Graham Loomis
Regional Trial Counsel
Georgia Bar No. 457868
Tel: (404) 842-7622
Email: loomism@sec.gov

COUNSEL FOR PLAINTIFF
Securities and Exchange Commission
Atlanta Regional Office
950 East Paces Ferry Road, N.E., Suite 900
Atlanta, GA 30326-1382
Tel (main): (404) 842-7600
Fax: (703) 813-9364