



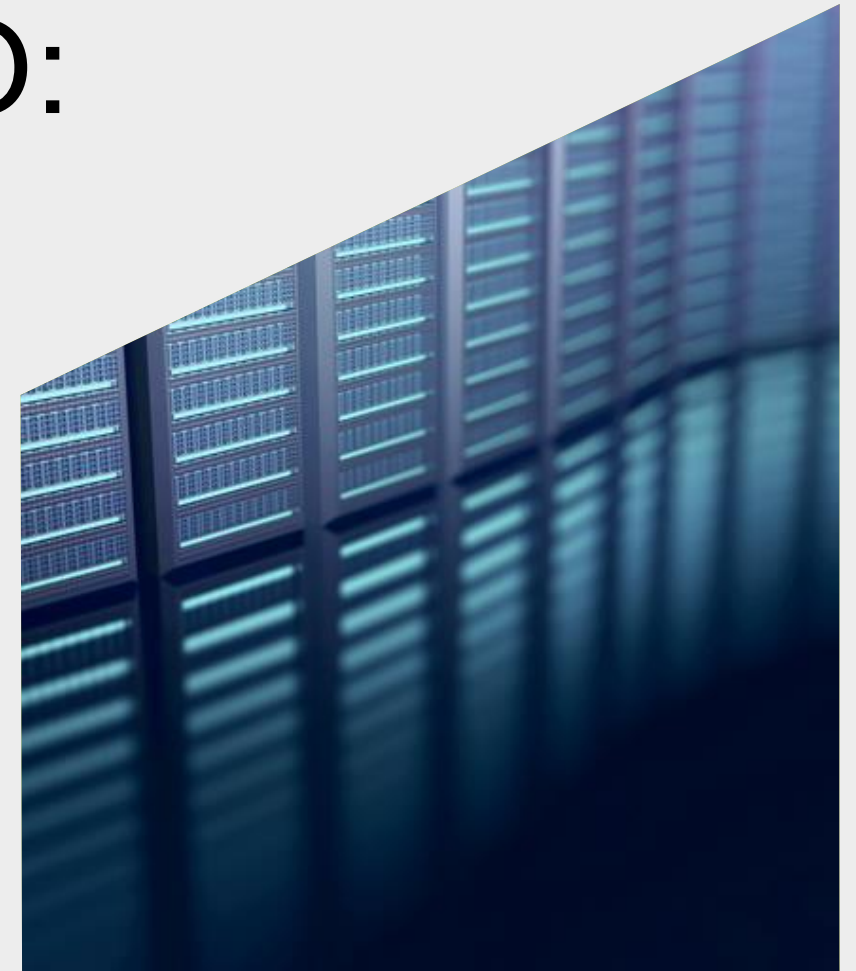
McDermott
Will & Emery

PROTECTING THE CISO:

A LEGAL JOURNEY

August 10, 2023

mwe.com



SPEAKERS



STEPHEN REYNOLDS
CISSP, CIPP/US

McDermott Will & Emery
Partner



NICK MERKER
CISSP, CIPT

Eli Lilly and Company
Associate Vice President, Assistant
General Counsel, Information Security
and Privacy

WHY DO SECURITY OFFICERS NEED PROTECTING?



LEGAL THREATS TO CISOs

UNITED STATES DISTRICT COURT

for the

Northern District of California

United States of America

v.

JOSEPH SULLIVAN

)
)
)
)
)
)
)

Case No. 3-20-71168 JCS

FILED

Aug 20 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

Defendant(s)

CRIMINAL COMPLAINT

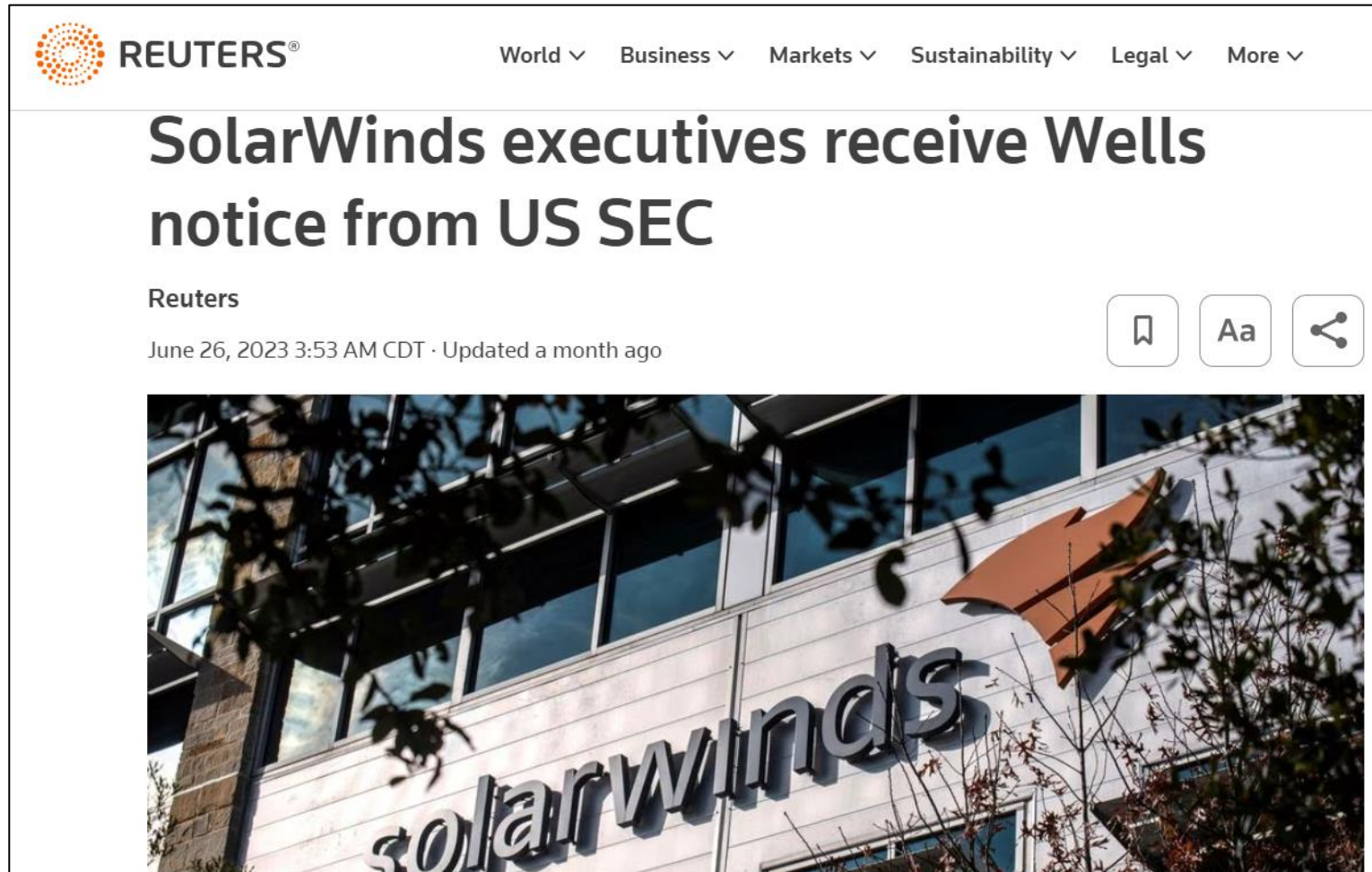
I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 15, 2016 to Nov. 21, 2017 in the county of San Francisco and elsewhere in the

Northern District of California, the defendant(s) violated:



LEGAL THREATS TO CISOs



LEGAL THREATS TO CISOs

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

SECURITIES AND EXCHANGE
COMMISSION,

v.

JUN YING,

Plaintiff, Securities and Exchange Commission
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.



IN-DEPTH REVIEW OF CASES



UNITED STATES V. SULLIVAN – THE CHARGES

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 15, 2016 to Nov. 21, 2017 in the county of San Francisco and elsewhere in the Northern District of California, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1505	Count One: Obstruction of Justice Max. Penalties: 5 years in prison; \$250,000 fine; 3 years of supervised release; \$100 special assessment; restitution; forfeiture
18 U.S.C. § 4	Count Two: Misprision of a Felony Max. Penalties: 3 years in prison; \$250,000 fine; 1 year of supervised release; \$100 special assessment; restitution; forfeiture



OBSTRUCTION OF JUSTICE

OBSTRUCTION OF PROCEEDINGS BEFORE
A DEPARTMENT OR AGENCY OF THE UNITED STATES
(18 U.S.C. § 1505)

The defendant is charged in Count One of the Superseding Indictment with obstructing a pending agency proceeding before the Federal Trade Commission or FTC, in violation of Section 1505 of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, there was a proceeding pending before a department or agency of the United States;

Second, the defendant was aware of the proceeding; and

Third, the defendant intentionally endeavored corruptly to influence, obstruct, or impede the pending proceeding.

The FTC is an agency of the United States, and an open or ongoing FTC investigation or matter constitutes a “pending proceeding” for the purposes of Title 18, United States Code, Section 1505.

MISPRISION OF A FELONY – TEXT OF STATUTE

18 U.S. Code § 4 - Misprision of felony

Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this title or imprisoned not more than three years, or both.

(June 25, 1948, ch. 645, 62 Stat. 684; Pub. L. 103-322, title XXXIII, § 330016(1)(G), Sept. 13, 1994, 108 Stat. 2147.)

MISPRISION OF A FELONY – JURY INSTRUCTION

The defendant is charged in Count Two of the Superseding Indictment with misprision of felony in violation of Section 4 of Title 18 of the United States Code. For the defendant to be found guilty of that crime, the government must prove each of the following elements beyond a reasonable doubt:

First, a federal felony was committed, that is, intentionally accessing a computer without authorization and thereby obtaining information from a protected computer, or conspiracy to extort money through a threat to impair the confidentiality of information obtained from a protected computer without authorization;

Second, the defendant had knowledge of the commission of that felony;

Third, the defendant had knowledge that the conduct was a federal felony;

Fourth, the defendant failed to notify a federal authority as soon as possible; and

Fifth, the defendant did an affirmative act to conceal the crime.



UNITED STATES V. SULLIVAN – KEY TESTIMONY

Craig Clark, then an attorney for Uber and another one of Sullivan’s reports, testified that after the response team learned that driver’s license numbers had been accessed, Sullivan asked him, “How can we fit this into bug bounty?”, which Clark understood to be a directive to find a way to bring the 2016 data breach within Uber’s bug bounty program—a type of program used by companies to incentivize outsiders to report vulnerabilities in the company’s security protocols. *See id.* at 498:8-13 (describing the nature of bug bounty programs); 732:9-733:13 (same); 1319:18-1320:24 (Clark’s testimony). According to Clark, Sullivan later told him that “we’re going to treat it as a bug bounty.” *Id.* at 1324:10-25.

UNITED STATES V. SULLIVAN – KEY TESTIMONY

One of the hackers testified that he negotiated with one of Uber’s employees for a payment of \$100,000—more than Uber’s typical maximum bug bounty payout of \$10,000—and in exchange, signed a non-disclosure agreement (“NDA”). *See id.* at 899:2-12; 965:13-19. The NDA stated that Uber would pay the hackers the \$100,000 if they promised that they “did not take or store any data during or through [their] research” and “delivered to [Uber] or forensically destroyed all information about and/or analyses of the vulnerabilities.” *See id.* at 900:5-901:16, 970:1-972:2. The NDA also required the hackers to promise that they “have not and will not disclose anything about the vulnerabilities or [their] dialogue with [Uber] to anyone for any purpose without [Uber’s] written permission.” *Id.* at 899:7-12. In exchange, the NDA promised



UNITED STATES V. SULLIVAN – KEY TESTIMONY

The jury was also presented with evidence, including the Preacher Central Tracker, that Sullivan and others at Uber believed that the circumstances of the 2016 data breach belied what he had previously told the FTC. *See, e.g.*, Ex. 29 at 11 (“This may also play very badly based on previous assertions.”); Tr. at 796:22-798:3 (testifying that this referenced “the FTC assertions” regarding data access and encryption); Ex. 29 at 18 (“Joe was just deposed on this specific topic and what the best or minimum practices that any company should follow in this area.”); Tr. at 629:1-630:6 (describing the statement). And it heard evidence about Sullivan’s efforts to keep the data breach a secret, including testimony from Sullivan’s direct report, John Flynn, who said that Sullivan told him “This can’t get out” when discussing the incident. *See* Tr. at 603:7-605:10; *see also id.* at 635:17-636:15 (discussing Preacher Central Tracker comments from Sullivan that “we



UNITED STATES V. SULLIVAN – KEY TESTIMONY

The second key piece of evidence is the NDA. The jury saw exhibits showing various edits made to the NDA that were attributed to Sullivan. *See, e.g.*, Exs. 100-115. It also heard testimony from Clark about the nature of those edits, including that specific language was “Joe’s idea,” and that when Clark noted the language was inaccurate, Sullivan told him “[t]hat it would stay.” *See* Tr. at 1344:16-1345:15.



UNITED STATES V. SULLIVAN – KEY TESTIMONY

The jury also heard evidence about steps that Sullivan took following the breach, which speak to the third and final element of the obstruction charge. Three pieces of evidence are key. First, the jury heard from Clark, who testified that after the response team learned that driver's license numbers had been accessed, Sullivan asked him, "How can we fit this into bug bounty?", which Clark understood to be a directive to find a way to fit the breach within Uber's bug bounty program. *Id.* at 1319:18-1320:24. Clark then testified that he developed a "theory" to avoid



UNITED STATES V. SULLIVAN – KEY TESTIMONY

Finally, the jury heard evidence regarding the \$100,000 payment made to the hackers, including testimony that at the time, Uber’s maximum bounty was \$10,000. *See id.* at 965:13-19. Later, one of Uber’s then-attorneys testified that Sullivan had said that the \$100,000 payment was “essentially to avoid the potential embarrassment to the company if it were to become disclosed.” *Id.* at 2176:5-14.

Sullivan makes much of the payment, arguing that there was insufficient evidence that he was responsible for it or that it was meant to impede the FTC investigation. *See Mot.* at 15:25-6:15. But, considered in the light most favorable to the prosecution and alongside the other

UNITED STATES V. SULLIVAN – VERDICT

We, the members of the Jury in this action, have reached the following unanimous verdict with respect to each Count of the Indictment:

Count One: (Obstruction of Proceedings Before a Department or Agency of the United States, in violation of 18 U.S.C. § 1505)

We find the defendant, Joseph Sullivan:

Guilty ✓ Not Guilty _____

Count Two: (Misprision of Felony, in violation of 18 U.S.C. § 4)

We find the defendant, Joseph Sullivan:

Guilty ✓ Not Guilty _____

UNITED STATES V. SULLIVAN – REST OF STORY

31. Soon after learning drivers' license numbers had potentially been exposed (at approximately 1:00am Pacific time on November 15, 2016), SULLIVAN reached out to Uber's then-CEO via text message. At approximately 1:28am on November 15, SULLIVAN sent the following text:

I have something sensitive I'd like to update you on if you have a minute.

32. Call records reflect that SULLIVAN and Uber's then-CEO had a series of conversations via phone and/or FaceTime lasting approximately five minutes. At approximately 1:38am, the CEO responded:

Need to get certainty of what he has, sensitivity/exposure of it and confidence that he can truly treat this as a bounty situation... resources can be flexible in order to put this to bed but we need to document this very tightly

SOLARWINDS CORPORATION SEC INVESTIGATION


SEC Investigation Update



As previously disclosed in the Company's Current Report on Form 8-K filed with the U.S. Securities and Exchange Commission (the "**SEC**") on November 3, 2022, on October 28, 2022, the enforcement staff of the SEC provided the Company with a "Wells Notice" relating to the SEC's investigation (the "**Investigation**") of the Cyber Incident. Subsequently, certain current and former executive officers and employees of the Company, including the Company's Chief Financial Officer and Chief Information Security Officer, received "Wells Notices" from the SEC staff, each in connection with the Investigation. The Wells Notices provided to these individuals each state that the SEC staff has made a preliminary determination to recommend that the SEC file a civil enforcement action against the recipients alleging violations of certain provisions of the U.S. federal securities laws.

Source: SolarWinds Corporation Form 8-K, dated June 23, 2023




SOLARWINDS CORPORATION SEC INVESTIGATION



Jamil Farshchi  • 1st
Equifax CISO | UKG Board Member | FBI Advisor
1mo • 

...

 Did the stakes just get monumentally raised for CISOs?

With the security industry focused on the fallout from MOVEit, Solarwinds (the OG of software supply chain risk) quietly dropped a bombshell of an 8K on Friday. 💣


Their CISO was served with a Wells Notice in connection with their 2020 cyber incident.

A Wells Notice says the SEC intends to recommend enforcement action against the individual for violating securities rules.

!! This is a really big deal.

It's unprecedented: this is likely the first time a CISO has ever received one of these.

And the implications are immense: Wells Notices are no joke. They create massive career hardships — especially if one plans to work for a publicly traded company.





SEC V. YING (EQUIFAX)

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

SECURITIES AND EXCHANGE
COMMISSION,

v.

JUN YING,

Plaintiff, Securities
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.

EQUIFAX

**U.S. House of Representatives
Committee on Oversight and Government Reform**



The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

EQUIFAX

2. Senior Equifax Employee Terminated for “Failing to Forward an Email”

On October 2, 2017, Equifax CIO for Global Corporate Platform terminated a highly-rated Equifax employee for failing to forward an email.

Payne told the Committee that he was not aware of the termination. When he pressed for more information, the employee refused to provide any documentation for the termination.



Figure 9: Former CEO Richard Smith Testifies before Congress (Oct. 3, 2017)

EQUIFAX – THE REST OF THE STORY...

Payne was just one of 430 employees to whom the GTVM email alert on the Apache Struts vulnerability was sent.³³⁶ Payne said he was copied on this email for informational purposes, but no specific action was required of him. He stated:

- A. So on the GTVM [email alert], I think all the CIOs were copied on that information. But, as I indicated, it was probably more for information than anything.
- Q. It wasn't necessary for action on your part?
- A. No, because I didn't have a responsibility under the [Patch Management] policy to – I wasn't a system owner or an application owner.³³⁷

Payne was never directed by anyone to forward such emails.³³⁸

MISSTATEMENTS / FRAUD

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

ALLIA
DALLA
TEXAS
behalf of
situated

ECL G

First, according to the Complaint, from March 22, 2021, through March 26, 2021,
despite knowing that it was experiencing service outages due to a ransomware attack, (ECF

No. 14 describing an unresolved ransomware attack as a mundane “technical issue” either pleads an
the ser outright false representation or at the very least the concealment of a material fact to hide from
caused Plaintiffs the true nature and severity of the situation surrounding the protection of their data.
attack i This same analysis applies to Plaintiffs’ additional allegations that Defendant used terms such
renderi as “performance issues,” (ECF No. 14 ¶ 61), “coding issues,” (*id.* ¶ 66), and “intermittent
[can] tl system issues,” (*id.* ¶ 83), during subsequent ransomware attacks.

HOW TO PROTECT YOUR CISO / YOURSELF



DIRECTORS AND OFFICER INSURANCE



DIRECTORS AND OFFICER INSURANCE

DIRECTORS, OFFICERS AND ENTITY LIABILITY

I. INSURING CLAUSES

- A. The Underwriters shall pay on behalf of the **Insured Persons** all **Loss** which is not indemnified by the **Insured Organization** resulting from any **Claim** first made against the **Insured Persons** and reported in writing to the Underwriters during the **Policy Period** or **Optional Reporting Period**, if applicable, for a **Wrongful Act**.
- B. The Underwriters shall pay on behalf of the **Insured Organization** all **Loss** which the **Insured Organization** is required or permitted to pay as indemnification to any of the **Insured Persons** resulting from any **Claim** first made against the **Insured Persons** and reported in writing to the Underwriters during the **Policy Period** or **Optional Reporting Period**, if applicable, for a **Wrongful Act**.

- J. **“Executive Officer”** means the chief executive officer, chief operating officer, president, **Manager**, chief financial officer, in-house general counsel, risk manager, or an individual acting in a similar capacity with the **Insured Organization**.

DIRECTORS AND OFFICER INSURANCE

III. EXCLUSIONS

The Underwriters shall not be liable to make any payment for **Loss** in connection with or resulting from any **Claim**:

- I. based upon, arising out of, directly or indirectly resulting from or in consequence of, or in any way involving:
 1. any deliberately dishonest, fraudulent or criminal act or omission by any of the **Insureds**; or
 2. any personal profit or advantage gained by any of the **Insured Persons** to which they were not legally entitled;as determined by a final non-appealable adjudication, except that this exclusion shall not apply to **Defense Costs** incurred up until such determination is made;



WHAT CAN YOU DO?



PRACTICAL TIPS



THANK YOU / QUESTIONS?

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein.

*For a complete list of McDermott entities visit mwe.com/legalnotices.

©2023 McDermott Will & Emery. All rights reserved. Any use of these materials including reproduction, modification, distribution or republication, without the prior written consent of McDermott is strictly prohibited. This may be considered attorney advertising. Prior results do not guarantee a similar outcome.

