UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

HAROLD LITWIN, Derivatively on behalf of T-MOBILE USA, INC.,

Plaintiff,

vs.

G. MICHAEL SIEVERT, TIMOTHEUS HÖTTGES, MARCELO CLAURE, SRIKANT M. DATAR, CHRISTIAN P. ILLEK, RAPHAEL KÜBLER, LETITIA A. LONG, THORSTEN LANGHEIM, DOMINIQUE LEROY, TERESA A. TAYLOR, OMAR TAZI, KELVIN R. WESTBROOK, MICHAEL WILKENS, and BAVAN M. HOLLOWAY,

Defendants,

-and-

T-MOBILE USA, INC.,

Nominal Defendant.

NO. 2:21-cv-1599

VERIFIED STOCKHOLDER DERIVATIVE COMPLAINT

JURY DEMAND

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Plaintiff Harold Litwin, by his undersigned attorneys, brings this stockholder derivative action in the name and on behalf of nominal defendant T-Mobile USA, Inc. ("T-Mobile" or the "Company") against the current members of the Company's Board of Directors (the "Board") for their breaches of fiduciary duties, violations of the federal securities laws, and other misconduct that resulted in material damage to the Company and its stockholders. These allegations are made upon personal knowledge with respect to Plaintiff and, as to all other matters, upon information and belief based upon the investigation and analysis by Plaintiff's counsel, including, among other things, a review of the Company's press releases and public filings with the United States Securities and Exchange Commission ("SEC"), corporate governance documents published on the Company's website, transcripts of T-Mobile investor conference calls, news reports, financial analyst reports, and other publicly available information about the Company. Plaintiff believes that substantial additional evidentiary support will exist for the allegations after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

1. This is a stockholder derivative action brought by Plaintiff on behalf of nominal defendant T-Mobile against the members of its Board (the "Individual Defendants") for their breaches of fiduciary duty, violations of the federal securities laws, and other misconduct that resulted in material damage to the Company and its stockholders.

2. T-Mobile is a telecommunications company. In the course of operating its core business, T-Mobile stores the personal identifying information of its millions of customers, making it a target for hackers and other malicious actors. The members of T-Mobile's Board were aware of the substantial risks posed to the Company, having recognized those very risks in public filings with the SEC and having assured stockholders that these risks were being properly managed.

3. The Individual Defendants, however, were long aware of red flags demonstrating

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

that the Company did not have an effective system of internal controls to ensure the safety and security of customers' personal identifying information in the face of this threat. Since 2015, hackers and other malicious actors have frequently exploited weaknesses in the Company's cybersecurity, from software bugs on the Company's website to unrestricted access on inadequately protected servers. Indeed, in February 2021, the Federal Communications Commission (the "FCC") levied a nearly $92 million fine on T-Mobile for its failure to protect customer location information and finding that the Company's privacy safeguards were "fundamentally weak."

4. The Defendants failed to heed the red flags demonstrating the lack of cybersecurity over customer data and repeatedly committed to do better next time, representing that data security was a priority at T-Mobile. The Defendants' failure caused substantial damage to the Company and its stockholders.

5. In August 2020, T-Mobile disclosed that customer personal identifying information for over 54 million[1] customers was accessed by a hacker. The FCC swiftly opened an investigation into T-Mobile, which remains ongoing. T-Mobile has also been subject to at least thirty-seven consumer class action lawsuits around the country based on the latest devastating cyberattack, alleging that T-Mobile has failed to adequately protect its millions of customers' valuable personal identifying information. *See, e.g., Daruwalla, et al. v. T-Mobile U.S. Inc.*, No. 2:21-cv-01118 (W.D. Wash. August 19, 2021); *Vash v. T-Mobile U.S. Inc.*, No. 1:21-cv-03384-SCJ (N.D. Ga. August 19, 2021); *Metzger v. T-Mobile U.S. Inc.*, No. 2:21-cv-04721-JMA-AYS (E.D.N.Y. August 20, 2021); *Peralta, et al v. T-Mobile U.S. Inc.*, No. 5:21-cv-00838-HE (W.D. Okla. August

[1] *See* Phil Muncaster, https://www.infosecurity-magazine.com/news/tmobile-breach-now-affects-546/ (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

24, 2021); *Savick v. T-Mobile U.S. Inc.*, No. 3:21-cv-16005-ZNQ-DEA (D.N.J. August 25, 2021); *Hill v. T-Mobile U.S. Inc.*, *No.* 2:21-cv-04164-NKL (W.D. Mo. August 25, 2021); *Winkler, et al. v. T-Mobile U.S. Inc.*, No. 7:21-cv-00322 (S.D. Tex. August 26, 2021); and *Lang v. T-Mobile U.S., Inc.*, No. 3:21-cv-06879-BLF (N.D. Cal. September 3, 2021). T-Mobile will now be subject to substantial costs defending itself in these investigations and lawsuits and is exposed to substantial liability.

6. Under the circumstances presented herein, demand is futile and, thus, excused. As directors, the Board was required to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal identifying information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders, and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal identifying information. The Board utterly failed to fulfill its fiduciary duties to the Company and its stockholders, each member faces a substantial likelihood of liability therefor, and a majority of the Board lacks independence.

7. In the absence of this action, T-Mobile will neither recover its damages nor properly remediate the weaknesses in its internal controls and corporate governance practices and procedures.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiff alleges claims arising under the laws of the United States. The Court has

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

supplemental jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a) because they are related to the claims arising under this Court's original jurisdiction and part of the same case or controversy. This action is not a collusive action designed to confer jurisdiction on a court of the United States that it would not otherwise have.

9. This Court has personal jurisdiction over each of the Defendants because each Defendant is either a corporation conducting business and maintaining operations in this District or is an individual who is either present in this District for jurisdictional purposes or has sufficient minimum contacts with this District so as to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391. T- Mobile maintains its principal executive offices in this District. Thus: (i) one or more of the Individual Defendants either resides or maintains executive offices in the District; (ii) a substantial portion of the transactions and wrongs complained of herein occurred in the District; and (iii) the Individual Defendants have received substantial compensation in the District by doing business and engaging in activities having an effect in the District.

III. PARTIES

A. Plaintiff

11. Plaintiff Harold Litwin is a long-term stockholder of T-Mobile and, as such, was a shareholder at the time of the transactions complained of herein.

B. Defendants

1. Nominal Defendant T-Mobile USA, Inc.

12. Nominal Defendant T-Mobile is a wireless network operator with headquarters in this district at 12920 Southeast 38th Street, Bellevue, WA 98006. T-Mobile's common stock

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

trades on the New York Stock Exchange ("NYSE") under the ticker symbol "TMUS." As of January 1, 2021, the Company had annual gross revenues of well over $60 billion.

2. Individual Defendants

a. Defendant Sievert

13. Defendant G. Michael Sievert ("Sievert") is President and Chief Executive Officer ("CEO") of T-Mobile and has served as a director since 2018. Sievert also served as the Company's Chief Operating Officer ("COO") from February 2015 to June 2018 and as President and COO from June 2018 to April 1, 2020. Sievert served in various other positions at the Company since November 2012.

14. As of March 31, 2021, Sievert beneficially owns 669,379 shares of the Company's stock. According to the Company's proxy statement filed with the SEC on April 21, 2021 (the "2021 Proxy Statement"), Defendant Sievert received the compensation outlined in the chart below over the past few years:

	Salary	Bonus	Stock Awards	Non-Equity Plan Compensation	Other Compensation	**Totals**
2020	$1,446,154	$3,500,000	$44,253,227	$5,600,000	$114,634	$54,914,014
2019	$1,200,000	N/A	$11,532,431	$3,576,000	$61,273	$16,369,704
2018	$1,108,654	N/A	$30,937,145	$3,592,039	$11,534	$35,649,372

b. Defendant Höttges

15. Defendant Timotheus Höttges ("Höttges") is Chairman of the Board of T-Mobile and has served as a director since 2013. Höttges serves as the Chair of the Executive Committee and Selection Committee. Höttges also serves as the CEO of Deutsche Telekom, a telecommunications company that controls over 52% of T-Mobile's voting stock. From March 2009 to December 2013, Höttges served as Deutsche Telekom's Chief Financial Officer and a

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

member of its Board of Management. Höttges has acted in various roles at Deutsche Telekom since 2006.

c. Defendant Claure

16. Defendant Marcelo Claure ("Claure") has served as a T-Mobile director since 2020 and is a member of its Compensation Committee, CEO Selection Committee, and Executive Committee. Claure also serves as the CEO of Softbank International and COO of Softbank. Claure served as a director of SoftBank from 2017 to 2020 and he currently serves as a director of Arm Limited and as Chairman of Brightstar Corporation ("Brightstar"), each a subsidiary of SoftBank. Claure was CEO of Brightstar until he left to join Sprint Corporation ("Sprint").[2]

17. As of March 31, 2021, Claure beneficially owns 7,034,791 shares of the Company's stock.

d. Defendant Datar

18. Defendant Srikant M. Datar ("Datar") has served as a T-Mobile director since 2013 and serves as Chair of its Audit Committee.

19. As of March 31, 2021, Datar beneficially owns 35,767 shares of the Company's stock. Defendant Datar received the compensation outlined in the chart below for serving as a T-Mobile director over the past few years:

	Fees earned or paid in cash	Stock Awards	Other Compensation	**Totals**
2020	$452,142	$297,824	$9,217	$759,183
2019	$212,701	$247,472	$5,274	$465,447
2018	$198,000	$178,798	$4,195	$380,993

[2] Claure served in various positions at Sprint, the last being Executive Chairman before Sprint merged with T-Mobile.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

e. Defendant Illek

20. Defendant Christian P. Illek ("Illek") has served as a T-Mobile director since 2018 and serves as Chair of its Compensation Committee and as a member of its Executive Committee and CEO Selection Committee. Illek has served as the Chief Financial Officer ("CFO") of Deutsche Telekom, T-Mobile's controlling stockholder, since January 2019. Since April 2015, Illek has served as a Member of Management Board of Deutsche Telekom. Illek has also served as Chairman of the Supervisory Board for T-Systems International GmbH since November 2016 (a subsidiary of Deutsche Telekom).

f. Defendant Kübler

21. Defendant Raphael Kübler ("Kübler") has served as a T-Mobile director since 2013 and is a member of its Compensation Committee and Executive Committee. Kübler has also served as the Senior Vice President of the Corporate Operating Office of Deutsche Telekom, T-Mobile's controlling stockholder, since 2014. From July 2009 to December 2013, Kübler served as Senior Vice President Group Controlling at Deutsche Telekom and was responsible for the financial planning, analysis and steering of the overall Deutsche Telekom Group as well as the financial management of central headquarters and shared services. From November 2003 to June 2009, Kübler served as Chief Financial Officer of T-Mobile Deutschland GmbH, the mobile operations of Deutsche Telekom in Germany (now a wholly owned subsidiary of Deutsche Telekom).

g. Defendant Long

22. Defendant Letitia A. Long ("Long") has served as a T-Mobile director since June 2021. Long also serves as a member of its Nominating and Corporate Governance Committee and as the Company's National Security Director in connection with T-Mobile's merger with Sprint.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Long also served as the former director of the National Geospatial-Intelligence Agency. Long has nearly 40 years of experience in security and intelligence.

h. Defendant Langheim

23. Defendant Thorsten Langheim ("Langheim") has served as a T-Mobile director since 2013 and is a member of its Compensation Committee, Executive Committee, and Selection Committee. Since 2009, Langheim has served in various roles at Deutsche Telekom, T-Mobile's controlling stockholder. Langheim joined the Board of Management of Deutsche Telekom in 2019, where he is responsible for the "USA and Group Development" Board department, overseeing Deutsche Telekom's U.S. business as well as corporate development, portfolio strategy and group M&A activities. This includes overseeing the management of Deutsche Telekom's subsidiaries T-Mobile Netherlands BV and Deutsche Funkturm. In addition, Langheim also serves as the Chairman and Co-founder of Deutsche Telekom Capital Partners, where he is responsible for the venture capital and private equity activities of Deutsche Telekom.

i. Defendant Leroy

24. Defendant Dominique Leroy ("Leroy") has served as a T-Mobile director since 2020 and is a member of its Nominating and Corporate Governance Committee. Leroy also serves as a member of the Board of Management of Deutsche Telekom, T-Mobile's controlling stockholder, since November 2020. Additionally, Leroy serves as a member of the board of directors of Hellenic Telecommunications Organization S.A., OTE Group ("Hellenic"), the largest telecommunications company in Greece.

j. Defendant Taylor

25. Defendant Teresa A. Taylor ("Taylor") has served as a T-Mobile director since 2013 and serves as the Chair of its Nominating and Corporate Governance Committee and as a

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

member of its Audit Committee and CEO Selection Committee. Taylor was designated by the Board as the lead independent director. Since April 2011, Taylor has served as CEO of Blue Valley Advisors, LLC, an advisory firm.

26. As of March 31, 2021, Taylor beneficially owns 28,222 shares of the Company's stock. Defendant Taylor received the compensation outlined in the chart below for serving as a T-Mobile director over the past few years:

	Fees earned or paid in cash	Stock Awards	Other Compensation	**Totals**
2020	$468,084	$297,824	$1,667	$767,575
2019	$224,771	$247,472	N/A	$472,183
2018	$193,250	$178,798	$11,217	$383,265

k. Defendant Tazi

27. Defendant Omar Tazi ("Tazi") has served as a T-Mobile director since 2020. Tazi is currently Senior Vice President at Deutsche Telekom, T-Mobile's controlling stockholder, in charge of Group Innovation, Products, Design & Customer Experience, as well as Global Partnerships and Devices.

l. Defendant Westbrook

28. Defendant Kelvin R. Westbrook ("Westbrook") has served as a T-Mobile director since 2013 and serves as the Chair of its Compensation Committee and as a member of its Audit Committee.

29. As of March 31, 2021, Westbrook beneficially owns 27,692 shares of the Company's stock. Defendant Westbrook received the compensation outlined in the chart below for serving as a T-Mobile director over the past few years:

	Fees earned or paid in cash	Stock Awards	Other Compensation	**Totals**
2020	$432,142	$297,824	$5,933	$735,899

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

2019	$204,242	$247,472	$3,809	$455,523
2018	$174,500	$178,798	$12,445	$365,743

m. Defendant Wilkens

30. Defendant Michael Wilkens has served as a T-Mobile director since 2020 and is a member of its Compensation Committee. Wilkens has served as Senior Vice President Group Controlling (FP&A) of Deutsche Telekom, T-Mobile's controlling stockholder, since October 2013. He joined Deutsche Telekom in 2001 and has since held various senior management positions in finance, as well as in international sales and marketing. Wilkens is a member of the board of directors of Hellenic and a member of the board of directors of T-Mobile Netherlands B.V. Additionally, he is a member of the advisory boards of T-Mobile Netherlands and Deutsche Telekom's Tower-Co business.

n. Defendant Holloway

31. Defendant Bavan M. Holloway ("Holloway") has served as a T-Mobile director since June of 2021. Holloway has over 30 years of finance and audit experience in complex and highly regulated business environments. Holloway previously was Vice President of Corporate Audit for Boeing, among other senior finance roles. She was also previously a Partner at KPMG International Limited.

IV. THE INDIVIDUAL DEFENDANTS' DUTIES

32. By reason of their positions as officers or directors of T-Mobile and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants owed T-Mobile and its shareholders fiduciary obligations of trust, loyalty, good faith, candor, due care, and diligence, and were and are required to use their utmost ability to control, manage, and oversee T-Mobile in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of T-Mobile and its shareholders so as

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

to benefit all shareholders equally and not in furtherance of their personal interests or benefit.

33. To discharge their duties, the officers and directors of T-Mobile were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the financial and corporate affairs and assets of the Company. By virtue of such duties, the directors of T-Mobile were required to, among other things:

a. review, approve, and oversee the implementation of the Company's major business, capital and financial objectives, strategy, and plans;

b. oversee the conduct of the Company's business by management;

c. oversee the Company's financial reporting and the integrity of its financial statements and internal control over financial reporting;

d. oversee the compensation of the CEO and other senior management of the Company;

e. perform an annual evaluation of the CEO;

f. assess Company risks and strategies for risk mitigation;

g. oversee the Company's legal and regulatory compliance and ethics policies; and

h. promote policies that encourage a corporate culture of openness, ethical conduct, honesty, fairness and accountability.

34. Each Individual Defendant, as a T-Mobile director, owed to the Company and to its shareholders the fiduciary duties of loyalty, good faith, due care and candor in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets.

A. Additional Duties Under The Code Of Ethics For Senior Financial Officers

35. Defendant Sievert, as CEO of the Company, is subject to additional duties under the Company's Code of Ethics for Senior Financial Officers (the "Code of Ethics").

36. Under the Code of Ethics, Sievert was obligated to adhere to, advocate, and

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

promote the following principles in addition to T-Mobile's Code of Conduct and other policies or guidelines that relate to the areas covered by the Code of Ethics:

- honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- full, fair, accurate, timely and understandable disclosure in reports and documents that T-Mobile files with, or submits to, the SEC and other regulatory authorities and in other public communications made by T-Mobile;
- compliance with laws, rules and regulations applicable to T-Mobile; and
- the prompt internal reporting of violations of the Code of Ethics.

37. The Code of Ethics further provides:

> The Audit Committee shall have the power to monitor, investigate, make determinations and recommend action to the Board of Directors with respect to violations of this Code of Ethics.

B. Additional Duties Under The Company's Code Of Business Conduct

38. The Code of Business Conduct stresses the role of leaders at the Company to set the tone, requiring that "they take care of problems before they become bigger problems . . . ."

39. The Code of Conduct provides that T-Mobile "take[s] care of" its customers, stressing that ***"[w]e earn the trust of our customers by putting them first every day."***[3]

40. The Code of Conduct emphasizes the importance of protecting the confidentiality of customer information, stating:

> Customers entrust a lot of sensitive information to us—credit card numbers, Social Security numbers, addresses, all sorts of things. We hold other customer information as well, like call detail records and location data. Here's the thing: We protect the confidentiality of our customers' information. We collect, use, and store this sensitive information only so far as is permitted by law, T-Mobile Terms & Conditions, and company Privacy policies.

41. The Code of Conduct further provides:

[3] All emphasis has been added unless otherwise noted.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> We demonstrate integrity 24/7. We're transparent. We do the right thing even when nobody is watching. Our business decisions are based on business factors and not personal interests. Period.

42. The Corporate Governance Principles provide that "[d]irectors must abide by the relevant provisions of the Company's Code of Business Conduct."

C. Additional Duties Under The Audit Committee Charter

43. The Audit Committee has certain additional duties as outlined in the Audit Committee Charter.

44. According to the Audit Committee Charter, the members of the Committee are obligated to:

- discuss policies with respect to risk assessment and risk management, including the Company's major financial risk exposures and the steps management has taken to monitor and control such exposures;
- prepare the report of the Committee required by the rules of the SEC to be included in the Company's annual proxy statement;
- develop and oversee compliance with a code of ethics for senior financial officers pursuant to and to the extent required by regulations applicable to the Company from time to time; and
- report regularly to the Board any issues that arise with respect to the quality and integrity of the Company's financial statements, the Company's compliance with financial, legal, statutory, and regulatory requirements, the performance and independence of the internal and independent auditors and the performance of the internal audit function.

D. Additional Duties Under The Nominating And Corporate Governance Committee Charter

45. The members of the Nominating and Corporate Governance Committee have additional duties under the Nominating and Corporate Governance Committee Charter (the "NCGC" Charter).

46. According to the NCGC Charter, the members of the Committee are obligated to:

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

- establish, coordinate, and review with the Chairman of the Board the criteria and methods for, at least annually, evaluating the effectiveness of the Board;
- develop and oversee a process for an annual evaluation of the Board;
- develop and oversee compliance with a Code of Business Conduct for all Company employees, officers and directors pursuant to and to the extent required by the rules of the NASDAQ Stock Market or any laws or regulations applicable to the Company from time to time;
- at least annually, review the implementation and effectiveness of the Company's compliance and ethics program with the Chief Compliance Officer;
- periodically review, and recommend to the Board appropriate revisions to, the Company's Corporate Governance Guidelines;
- develop and recommend to the Board for approval such other corporate governance policies as the Committee determines necessary or appropriate, and periodically review and recommend to the Board appropriate revisions to such other corporate governance policies; and
- monitor compliance with and the effectiveness of the aforementioned Code and Company Speak Up Policy, and Corporate Governance Guidelines, except to the extent that such responsibility has been assigned to another committee of the Board.

V. SUBSTANTIVE ALLEGATIONS

A. T-Mobile Collects And Stores Confidential Personal Data From Customers

47. T-Mobile is a telecommunications company that provides mobile communication services, among other products and services, throughout the United States and internationally. According to the Company's Annual Report on Form 10-K filed with the SEC on February 23, 2021 for the period ending December 31, 2020 (the "2020 10-K"), the Company "provide[s] wireless services to 102.1 million postpaid and prepaid customers and generate[s] revenue by providing affordable wireless communications services to these customers, as well as a wide selection of wireless devices and accessories."

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

48. The Company collects data in the ordinary course of business and stores that data on its servers. According to the Company's Privacy Notice,[4] some of the personal and confidential information that T-Mobile collects from its customers and potential customers includes:

- Name
- Address
- E-Mail Address
- Phone number
- Government identification number
- Social Security number
- Security codes
- Signature
- Date of Birth
- Payment information (such as credit and debit cards, and bank account numbers).

49. The Company states in the Privacy Notice that it protects customer data:

> We use administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control. For example, when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access.

50. T-Mobile also collects data on its customer and potential customer base from other sources such as shippers, financial institutions, and credit agencies and through analyzing customer use of its products and services.

[4] *See* https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited on October 11, 2021). The Privacy Notice cited was effective on May 5, 2021.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

51. The substantial amount of confidential customer data collected by T-Mobile "makes them a target" of hackers and other malicious actors.[5] As such, the Company represents[6] that its "job is to come up with foolproof data security":

> Our network is vast. Our customers number in the millions. And we want their data safe. ***Our job is to come up with foolproof cybersecurity solutions*** for mobile devices, security automation, 5G, IoT and more. At T-Mobile, there's room for only one kind of cybersecurity professional: the best kind.

B. The Individual Defendants Knew Of Substantial Cybersecurity Risks

52. In the 2020 10-K, a majority of the Individual Defendants[7] acknowledged the substantial risks that data loss or security breaches pose to the Company:

> **We could be harmed by data loss or other security breaches, whether directly or indirectly.**
>
> Our business involves the receipt, storage and transmission of our customers' confidential information, including sensitive personal information and payment card information, confidential information about our employees and suppliers, and other sensitive information about our Company, such as our business plans, transactions and intellectual property (collectively, "Confidential Information"). Unauthorized access to Confidential Information may be difficult to anticipate, detect, or prevent, particularly given that the methods of unauthorized access constantly change and evolve. ***We are subject to the threat of unauthorized access or disclosure of Confidential Information by state-sponsored parties, malicious actors, third parties or employees, errors or breaches by third-party suppliers, or other security incidents that could compromise the confidentiality and integrity***

---

[5] *See David Uberti*, https://www.wsj.com/articles/t-mobile-faces-regulatory-scrutiny-after-hack-11629401366 (last visited on October 11, 2021) (quoting Susan Welsh de Grimaldo, an analyst at research firm Gartner Inc).

[6] *See* https://www.t-mobile.com/careers/digital-security (last visited October 11, 2021).

[7] The 2020 10-K was signed by Defendants Sievert, Höttges, Claure, Datar, Illek, Kübler, Langheim, Leroy, Taylor, Tazi, Westbrook, and Wilkens. Pursuant to the Sarbanes-Oxley Act of 2002 ("SOX"), Defendant Sievert certified that the 2020 10-K fully complied with the requirements of section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that the information contained in the 2020 10-K fairly presented, in all material respects, the financial condition and results of operations of the Company.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> ***of Confidential Information****. . . . [W]e expect to continue to be the target of cyber-attacks, data breaches, or security incidents, which may in the future have a material adverse effect on our business, reputation, financial condition, and operating results.*

53. The Company also acknowledged in the 2020 10-K that because of its role as a communications carrier and its connections to third-party service providers, it was more likely to be the target of an attack:

> As a telecommunications carrier, we are considered a critical infrastructure provider and therefore ***may be more likely to be the target of cyber-attacks*** (e.g., denial of service and other malicious attacks). Such attacks against companies may be perpetrated by a variety of groups or persons, including those in jurisdictions where law enforcement measures to address such attacks are ineffective or unavailable, and such attacks may even be perpetrated by or at the behest of foreign governments.
>
> In addition, we provide confidential, proprietary and personal information to third-party service providers as part of our business operations. These third-party service providers have experienced data breaches and other attacks that include unauthorized access to Confidential Information in the past, and face security challenges common to all parties that collect and process information.

54. In the 2020 10-K, it is recognized that future data breaches may have a material adverse effect on T-Mobile's business, financial condition and operating results:

> Our procedures and safeguards to prevent unauthorized access to sensitive data and to defend against attacks seeking to disrupt our services must be continually evaluated and revised to address the ever-evolving threat landscape. . . . If we or our third-party suppliers are subject to such attacks or security breaches, we may incur significant costs or other material financial impacts, which may not be covered by, or may exceed the coverage limits of, our cyber insurance, ***be subject to regulatory investigations, sanctions and private litigation***, ***experience disruptions to our operations or suffer damage to our reputation. Any future cyber-attacks, data breaches, or security incidents may have a material adverse effect on our business, financial condition and operating results.***

55. The 2020 10-K also discusses the risk of unauthorized access to T-Mobile and related third party servers and the theft of customers' personal information:

> To be successful, we must provide our customers with reliable, trustworthy service ***and protect the communications, location, and personal information shared or***

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> ***generated by our customers.*** We rely upon systems and networks - those of suppliers and other providers, in addition to our own - to provide and support our services and, in some cases, protect our customers' information and our information. System, network or infrastructure failures may prevent us from providing reliable service or may allow for unauthorized use of or interference with our networks and other systems or the compromise of customer information. Examples of these risks include:
>
> - ***theft of customer and/or proprietary information offered for sale for competitive advantage or corporate extortion; [and]***
> - ***unauthorized access to our IT and business systems or to our network and critical infrastructure and those of our suppliers and other providers.***

56. In the 2020 10-K, the Company also discusses the threat of cyberattacks in connection with its merger with Sprint, stating as follows:

> Following the closing of the Merger, we are operating and maintaining multiple billing systems. We expect to continue to do so until successful migration of Sprint's legacy customers to T-Mobile's existing billing platforms. We may encounter unanticipated difficulties or experience delays in the ongoing integration efforts with respect to billing, causing major system or business disruptions. ***In addition, we or our supporting vendors may experience errors, cyber-attacks or other operational disruptions that could negatively impact us and over which we may have limited control.*** Interruptions and/or failure of these billing systems could disrupt our operations and impact our ability to provide or bill for our services, retain customers, **attract** new customers or negatively impact overall customer experience. Any occurrence of the foregoing could cause material adverse effects on our operations and financial condition, and/or material weaknesses in our internal control over financial reporting and reputational damage.

C. Federal And State Laws Require Companies That Store Personal Identifying Information To Protect That Information

1. Duties Under the Communications Act

57. The Communications Act of 1934[8] ("Communications Act"), as amended, details privacy protection obligations for telecommunications carriers, such as T-Mobile.

58. Section 222 of the Communications Act begins as follows:

---

[8] Pub. L. 117-38, 47 USCS § 222.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> **(a) In general.** Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

59. Section 222 further provides:

> **(c) Confidentiality of customer proprietary network information.**
>
> **(1)** Privacy requirements for telecommunications carriers. Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

2. Duties Under Washington State Law

60. A recent Washington State law expands the notification requirements relating to data breaches that expose personal customer information.

61. Signed into law on May 7, 2019, and effective on March 1, 2020, H.B. 1071 requires that:

> Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured.

62. H.B. 1071 further requires that:

> Any person or business that maintains or possesses data that may include personal information that the person or business does not own or license shall notify the owner or licensee of the information of any breach of the security of the data ***immediately following discovery***, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

63. H.B. 1071 further expands the mandated content for a data breach notification by requiring that notice to affected individuals includes, among other details, "***a time frame of exposure of the relevant personal information, if known, including the date of the breach and***

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

the date of discovery of the breach."[9]

64. Further, notice made to the Attorney General[10] must include additional content, including a list of the types of information affected by the breach, the time frame of exposure (including the date of the breach and the date the breach was discovered), a summary of steps taken to contain the breach and a sample copy of the notice to affected individuals.[11]

65. Based on the new requirements under H.B. 1071, the Washington State Office of the Attorney General recommends that a business take the following steps[12] to ensure compliance with the law, *inter alia*:

- Assess whether you truly need to collect and store the "personal information" that is being held.
- Develop policies for the collection, encryption, and use of "personal information."
- Ensure your business or agency has an action plan in the event of a data breach.
- ***Develop a dedicated Incident Response Team, or implement automated security technologies to detect attempted breaches.***

3. Duties Under New York State Law

66. New York State has recently enacted a new law relating to protecting customers' personal information, the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act").[13]

---

[9] *See* H.B. 1071 Sec. 2 (6) (b) (iii).

[10] The law obligates the entity to inform the Attorney General, if the breach affects more than 500 Washington residents.

[11] *Id.*

[12] *See* https://www.atg.wa.gov/hb1071-faq#question8 (last visited October 11, 2021).

[13] *See* NY CLS Gen. Bus. § 899-bb.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

67. The SHIELD Act, which took effect on March 21, 2020, significantly broadened the scope of New York's original data breach notification law.[14]

68. In particular, the SHIELD Act expands the safeguards required for any person or business handling New York residents' private information.

69. The SHIELD Act states as follows:

> 2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York ***shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.***

To comply with the above section of the SHIELD Act, the person or business must implement a data security program that has the following administrative, technical, and physical safeguards:

- designates one or more employees to coordinate the security program;
- identifies reasonably foreseeable internal and external risks;
- ***assesses the sufficiency of safeguards in place to control the identified risks***;
- trains and manages employees in the security program practices and procedures;
- ***selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract***;
- ***adjusts the security program in light of business changes or new circumstances***;
- assesses risks in network and software design;
- assesses risks in information processing, transmission and storage;
- detects, prevents and responds to attacks or system failures;
- regularly tests and monitors the effectiveness of key controls, systems and procedures;
- assesses risks of information storage and disposal;

[14] *Id.*

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

- ***detects, prevents and responds to intrusions***;
- protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- disposes of private information within a reasonable amount of time ***after it is no longer needed for business purposes*** by erasing electronic media so that the information cannot be read or reconstructed.

70. The SHIELD Act also states that notification to consumers of "unauthorized access" is required even where that intrusion did not lead to the acquisition of private information.[15]

D. The Individual Defendants Failed To Heed Red Flags Demonstrating T-Mobile's Lack Of Cybersecurity

71. Despite the Company's oft-repeated commitment to data security, "[u]nfortunately, dealing with data breaches is nothing new for the company—or its customers."[16] T-Mobile customers have been victimized in numerous data breaches in recent years.[17]

72. In 2015, T-Mobile customer data was exposed in the data breach perpetrated on Experian Information Solutions, Inc. ("Experian"). The information accessed included name, address and birthdate as well as encrypted fields with Social Security numbers and ID numbers (such as driver's license or passport numbers), and additional information used in T-Mobile's own

---

[15] *See* NY CLS Gen. Bus. § 899-aa ("'Breach of the security of the system' ***shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization***, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business . . . .").

[16] *See* Chris Velazco, *Here's what to do if you think you're affected by T-Mobile's big data breach*, WASHINGTON POST, https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/ (last visited October 11 2021).

[17] *See* Dan Goodin, https://arstechnica.com/gadgets/2021/08/t-mobile-has-been-hacked-yet-again-but-still-doesnt-know-what-was-taken/ (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

credit assessments.[18] Then T-Mobile CEO, John Legere ("Legere"), stated that he was "incredibly angry" about the data breach and assured that he took "our customer and prospective customer privacy VERY seriously." Legere represented that the Company was serious about data security as well stating that "[a]t T-Mobile, privacy and security is of utmost importance."[19]

73. Following the Experian breach, T-Mobile's response was offering T-Mobile customers two years of free credit monitoring and identity protection through Experian, the company that had just been breached.

74. In 2017, Karan Saini ("Saini"), a security researcher discovered a bug on a T-Mobile website that allowed hackers access to personal data such as email addresses, account numbers, and the phone's IMSI, a standardized unique number that identifies subscribers.[20] Before the bug in T-Mobile's website was uncovered by Saini, hackers found it, used it for several weeks, and even uploaded a tutorial to YouTube on how to exploit it, all without T-Mobile stepping in to protect customer data. According to Saini, the bug let hackers "scrape the data" from all of the Company's customers, over 74 million people. Saini warned that the breach "very critical."

75. T-Mobile claimed to have quickly patched the bug, but in August 2018, T- Mobile disclosed that hackers accessed personal information relating to two million customers.[21] T- Mobile assured that the cybersecurity team had shut down the unauthorized access and that the

---

[18] *See* https://www.t-mobile.com/news/blog/experian-data-breach (last visited October 11, 2021).

[19] *Id.*

[20] *See* Lorenzo Franceschi-Biccieral, MOTHERBOARD, https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number (last visited October 11, 2021).

[21] *See* https://www.t-mobile.com/customers/6305378821 (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Company had "promptly reported it to authorities." The Company revealed that certain personal information of its customers was accessed by the hackers:[22]

> None of your financial data (including credit card information) or social security numbers were involved, and no passwords were compromised. However, you should know that some of your personal information may have been exposed, which may have included one or more of the following: name, billing zip code, phone number, email address, account number, account type (prepaid or postpaid), and/or date of birth.

76. The Company promised that it would get it right next time, stating:

> We take the security of your information very seriously and have a number of safeguards in place to protect your personal information from unauthorized access. We truly regret that this incident occurred and are so sorry for any inconvenience this has caused you.

77. In November 2019, T-Mobile again disclosed to customers that its cybersecurity team "discovered and shut down malicious, unauthorized access to some information related to your T-Mobile prepaid wireless account."[23] The exposed data included personal information such as customer names, billing addresses, phone numbers, account numbers, rate plans, and plan features.

78. In March 2020, T-Mobile revealed once again that it was subject to a data breach that exposed customer and employee personal information, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers, and billing account information.[24] T-Mobile did not say how many users were impacted

---

[22] *Id*.

[23] *See* Catalin Cimpanu, ZDNET, https://www.zdnet.com/article/t-mobile-discloses-security-breach-impacting-prepaid-customers/ (last visited October 11, 2021).

[24] *See* Catalin Cimpanu, ZDNET, https://www.zdnet.com/article/t-mobile-says-hacker-gained-access-to-employee-email-accounts-user-data/ (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

but recommended that customers change the personal identification number on their T-Mobile accounts.

79. In late 2020, T-Mobile again suffered a data breach in which hackers accessed customer proprietary network information (CPNI) and undisclosed call-related information for hundreds of thousands of customers.[25] The Company disclosed to customers that the CPNI information possibly "included phone numbers, number of lines subscribed to on your account and, in some cases, call-related information collected as part of the normal operation of your wireless service."

80. On February 28, 2021, the FCC levied a $91.6 million fine[26] on T-Mobile for violating section 222 of the Communications Act and the FCC's regulations governing the privacy of customer information when T-Mobile failed to protect customer location information.[27] The fine was imposed after an investigation by the FCC following an incident where a Missouri law enforcement official was able to get customer location information from the servers of Securus Technologies, Inc. ("Securus"), which bought the information from the major communication

[25] *See* Alicia Hope, *CPO Magazine*, Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers - CPO Magazine https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/ (last visited October 11, 2021).

[26] Sprint, Verizon, and AT&T also were fined significant amounts, but the largest such fine was levied against T-Mobile.

[27] *See* the Company's 2020 10-K, pg. 30. *See also* https://www.fcc.gov/document/fcc-proposes-916m-fine-against-t-mobile-location-information-case (last visited October 11, 2021). *See also* https://incompliancemag.com/u-s-fcc-proposes-200-million-fine-for-failure-to-protect-consumer-location-data/ (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

carriers, such as T-Mobile, through third parties, without the consent of customers.[28] The FCC Enforcement Bureau reached out to Lisa Lancetti, Chief Counsel at T-Mobile, on numerous occasions to obtain documents and other information relating to the investigation. *See* Notice of Apparent Liability for Forfeiture and Admonishment, ¶ 38.

81. In the FCC's Notice of Apparent Liability for Forfeiture and Admonishment[29] that accompanied the fine, the FCC stated:

> In plain terms, our rules recognize that companies cannot prevent all data breaches, but require carriers to take ***reasonable steps*** to safeguard their customers' CPNI and to discover attempts to gain access to their customers' CPNI.
>
> ***
>
> The Securus incident ***laid bare the fundamental weaknesses of T-Mobile's safeguards with respect to the third parties to which it entrusted its customers' location information***.

E. Over 54 Million T-Mobile Customers' Personal Information Is Stolen By Hackers

82. On or about August 15, 2021, T-Mobile was reported to be "investigating a forum post claiming to be selling a mountain of personal data" obtained from T-Mobile servers.[30] The

---

[28] The FCC referred to the incident as the "Securus incident." Securus, a provider of telecommunications services to correctional facilities throughout the United States, also operated a "location-finding service" that enabled law enforcement and corrections officials to access the location of a mobile device belonging to customers of major wireless carriers, *without* the device owner's knowledge or consent. *See* Notice of Apparent Liability for Forfeiture and Admonishment, ¶ 27, https://www.fcc.gov/document/fcc-proposes-916m-fine-against-t-mobile-location-information-case (last visited October 11, 2021.)

[29] *See* https://www.fcc.gov/document/fcc-proposes-916m-fine-against-t-mobile-location-information-case (last accessed on October 11, 2021).

[30] *See, e.g.*, Joseph Cox, VICE, https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

forum post did not mention T-Mobile, but the seller reached out to media sources claiming to possess personal data of over 100 million people from T-Mobile servers. The data stolen included social security numbers, phone numbers, names, physical addresses, unique IMEI[31] numbers, and driver license information.[32]

83. The forum post offered to sell a subset of the data containing 30 million social security numbers and driver licenses for six bitcoins, at the time worth approximately $270,000. The forum post indicated that the rest of the data was being sold privately.[33] At the time, T-Mobile said it was investigating the reports and declined to answer follow-up questions from the media about the scale of the breach.[34]

84. On August 16, 2021, T-Mobile admitted that there had been a data breach, but said it was still investigating if any personal customer information had been stolen. The Company said it was confident it had closed the access point and that it was continuing its technical review of the situation to identify the nature of any data that was illegally accessed.[35]

---

[31] IMEI (International Mobile Equipment Identity) is a 15-17-digit code that is given to every mobile phone. This number is used by service providers to uniquely identify valid devices. Having your IMEI number hacked is a serious matter since you could face a service interruption with your own smartphone or cell phone, and it's also possible that thieves could access your personal information to commit ID fraud. *See* https://whatis.techtarget.com/definition/IMEI-International-Mobile-Equipment-Identity; https://www.phonecheck.com/blog/how-to-check-imei-number-hacked (last visited October 10, 2021).

[32] *See, e.g.*, Joseph Cox, VICE, https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last visited October 11, 2021).

[33] *Id.*

[34] *Id.*

[35] *See* Michael Hill, CSO, https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

85. The data breach, a "particularly massive one,"[36] caused T-Mobile's stock to drop about three percent, closing at $140.73 per share at the end of trading on August 16.

86. On August 17, T-Mobile issued an update on its investigation into the data breach and confirmed that the data stolen contained customers' personal information:

> We have no indication that the data contained in the stolen files included any customer financial information, credit card information, debit or other payment information. ***Some of the data accessed did include customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of current and former postpaid customers and prospective T-Mobile customers***.[37]

87. The Company stated that approximately "7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile" along with "850,000 active T-Mobile prepaid customer names, phone numbers, and account PINs [which] were also exposed."[38]

88. T-Mobile offered two years of identity protection services with McAfee's ID Theft Protection Service to effected customers and advised that all T-Mobile postpaid customers should change their PIN.

89. On August 18, 2021, security researcher Brian Krebs warned that T-Mobile customers will not only have to worry about their data in the hands of malicious actors, but they would likely face phishing attacks and harassment after the data breach:

---

[36] *See* Nicholas Jasinski, BARRON'S, https://www.barrons.com/articles/customer-data-breach-reports-t-mobile-stock-51629130492 (last visited October 11, 2021).

[37] *See* Michael Hill, CSO, https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html (last visited October 11, 2021).

[38] *See* https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> T-Mobile customers should expect to see phishers taking advantage of public concern over the breach to impersonate the company — and possibly even messages that include the recipient's compromised account details to make the communications look more legitimate.[39]

90. On August 20, 2021, T-Mobile disclosed that it had discovered that another 5.3 million existing customers and 667,000 former customers were affected by the breach:

> Additionally, we have since identified another 5.3 million current postpaid customer accounts that had one or more associated customer names, addresses, date of births, phone numbers, IMEIs and IMSIs illegally accessed. These additional accounts did not have any SSNs or driver's license/ID information compromised.
>
> ***
>
> Separately, we have also identified further stolen data files including phone numbers, IMEI, and IMSI numbers. That data included no personally identifiable information.
>
> We continue to have no indication that the data contained in any of the stolen files included any customer financial information, credit card information, debit or other payment information.[40]

91. T-Mobile's August 20, 2021 disclosure brought the total number of people affected by the data breach to at least 54.6 million.[41]

92. In an article published in *Inc.* a few days following the massive data breach, tech columnist, Jason Aten, reported that T-Mobile's response to the data breach was the one thing "no company should ever do."[42] The article first points out that the only way that T-Mobile learned of

---

[39] *Id.*

[40] *See* https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited October 11, 2021).

[41] *See* Shannon Stapleton, REUTERS, https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/ (last visited October 11, 2021). *See also* Phil Muncaster, https://www.infosecurity-magazine.com/news/tmobile-breach-now-affects-546/ (last visited October 11, 2021).

[42] *See* https://www.inc.com/jason-aten/t-mobile-data-breach-50-million-accounts-how-to-

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

the breach was through the media reports of the seller's forum post. T-Mobile failed to detect the breach through its cybersecurity monitoring procedures and was forced to play catch-up after learning of the intrusion from the media. The article noted that T-Mobile's reassurance that "no financial information or credit or debit card information" was compromised was illusory because a person with bad intentions had access to all of the other personal data needed to simply open a credit card in the victim's name.

93. Aten stressed that T-Mobile's text message sent out to some customers was confusing because it grossly understated the extent of the breach and left customers who received no communication wondering if their personal information was safe. "Just because you have 'no information' that a specific customer's SSN has been compromised, in this case, it's probably a best practice to assume it was and act accordingly." Aten noted that "I'm a T-Mobile customer, and I've yet to receive a single communication from the company about the breach. Does that mean my information is safe? It's hard to know."

94. Aten found that T-Mobile failed to protect its customers' personal information and lacked transparency:

> As for the companies we give our information to, we expect them to protect that data. That's not unreasonable. Also not unreasonable is an expectation that if someone steals our information, those companies should be upfront and transparent about what happened, what they are doing about it, and what steps we need to take. If you can't protect our information, at least tell us what we need to do to protect ourselves.
>
> T-Mobile's blog post says all the right words. For example, it explains that the company is "relentlessly focused on taking care of our customers -- that has not changed. We've been working around the clock to address this event and continue protecting you, which includes taking immediate steps to protect all individuals who may be at risk."

---

protect-yourself.html (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> Except, if you're relentlessly focused on taking care of your customers, communication is pretty important. That's true all the time, but especially when their personal information is at risk.

95. Martin Riley, director of managed security services at Bridewell Consulting, stated[43] that it was concerning that T-Mobile only discovered the illegal access after a malicious actor started selling stolen customer data online:

> The problem is that working out what has been taken, and when, can be very challenging for many organizations which is why the average breach detection and containment time is still so long.
>
> Enterprises need to shift from a security monitoring and notification approach to one focused on threat detection and response. T-Mobile has been subject to numerous attacks in the past few years and needs to act competently and confidently to minimize reputational damage or a decline in public confidence.

96. On August 26, in an interview with *The Wall Street Journal*, a twenty-one-year- old American man living in Turkey, John Binns ("Binns"), claimed to be responsible for the data breach.[44] According to the report, Binns represented that he initially gained access to T-Mobile's network in July through an unprotected router. The article quoted Binns as saying that "I was panicking because I had access to something big. ***Their security is awful.***" Binns also said that he spent about a week rummaging through T-Mobile's servers.

97. On August 27, Defendant Sievert published a public letter[45] on the Company's website apologizing for the massive data breach. Sievert admitted that "we didn't live up to the expectations we have for ourselves to protect our customers," and that "[k]nowing that we failed

---

[43] *See* Phil Muncaster, https://www.infosecurity-magazine.com/news/tmobile-breach-now-affects-546/ (last visited October 11, 2021).

[44] *See* Michael Hill, CSO, https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html (last visited October 11, 2021).

[45] *See* https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

to prevent this exposure is one of the hardest parts of this event."

98. Defendant Sievert also admitted in the letter that the Company's cybersecurity needed an overhaul remarking that "[w[e know we need additional expertise to take our cybersecurity efforts to the next level…."

99. In a *Verge* article,[46] tech columnist, Richard Lawler commented on Sievert's belated apology and T-Mobil's commitment to get it right this time around:

> To do something about it, T-Mobile is partnering with cybersecurity firm Mandiant and consultants at KPMG to tighten things up. Will that put an end to this ***ridiculous streak of insecurity***? No one can know, but that's more than the "sorry for any inconvenience" notes released after some of the past breaches, and of course, all the subscribers got a free year of Apple TV Plus.[47] Too bad it's only happening after a hacker made off with enough IMEI/IMSI, driver's license, and social security data to spend the next few years stealing identities and phone numbers at will.

F. T-Mobile Is Under Investigation By The FCC And The FBI

100. Shortly after the discovery of the enormous breach, the FCC started an investigation into the massive hack of T-Mobile.[48] An FCC spokeswoman said, "Telecommunications companies have a duty to protect their customers' information."[49]

101. Amy Keller ("Keller"), the leader of the cybersecurity and technology law group

---

[46] *See* https://www.theverge.com/2021/8/28/22646439/t-mobile-data-breach-ceo-security-mandiant-kpmg (last visited October 11, 2021).

[47] *See* Chaim Gartenberg, Verge, https://www.theverge.com/2021/8/23/22637797/tmobile-free-apple-tv-plus-12-months-magenta-plans (last visited October 11, 2021).

[48] *See* BLOOMBERG LAW, https://news.bloomberglaw.com/privacy-and-data-security/fccs-t- mobile-probe-is-early-sign-of-democrats-privacy-stance (last visited October 11, 2021).

[49] *See* David Uberti, *The Wall Street Journal*, https://www.wsj.com/articles/t-mobile-faces-regulatory-scrutiny-after-hack-11629401366 (last visited October 11, 2021).

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

at Dicello Levitt Gutzler stated that T-Mobile's practice of storing customers' data raised questions at the FTC and other agencies regarding the Company's security practices.[50] Keller pointed out that it was questionable why T-Mobile needed to keep prospective customers' social security and driver's license information stored on its servers when "[t]hese people didn't even sign an agreement with T-Mobile."[51]

102. The Seattle office of the Federal Bureau of Investigation ("FBI") was also reported to be investigating the T-Mobile data breach.[52]

G. T-Mobile Is Sued In Numerous Consumer Class Action Lawsuits

103. In the wake of the Company's disclosure of the massive data breach, T-Mobile was sued in at least thirty-seven consumer class action lawsuits filed in courts all around the country. The lawsuits focus on T-Mobile's responsibility as a communications carrier handling millions of consumers' valuable personally identifiable information[53] and the Company's failure to meet their obligation to protect sensitive information entrusted to them by their current and former customers.

104. A nationwide class of T-Mobile consumers[54] affected by the massive August 2021 data breach brought at least twenty-one class actions against the Company in Washington State

---

[50] *Id.*

[51] *Id.*

[52] *See* Joe Dyton, CONNECTED, https://connectedremag.com/das-in-building-wireless/wireless/t-mobile-ceo-offers-apologies-for-recent-data-breach/ (last visited on October 11, 2021).

[53] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79.

[54] The lawsuits have additional state specific subclasses along with the nationwide class.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

seeking compensation for their damages under principles of common law negligence, unjust enrichment, breach of contract, and based on other state-specific laws.[55] The Washington class actions also seek declaratory and injunctive relief. *See, e.g., Daruwalla, et al. v. T-Mobile U.S. Inc.*, No. 2:21-cv-01118 (W.D. Wash. August 19, 2021).

105. A nationwide class of T-Mobile consumers[56] brought at least five lawsuits against the Company in the District Court of New Jersey seeking compensation, injunctive and declaratory relief under claims of negligence, breach of implied contract, breach of confidence, breach of fiduciary duty, invasion of privacy, and breach of the covenant of good faith and fair dealing. *See, e.g., Savick v. T-Mobile U.S. Inc.*, No. 3:21-cv-16005-ZNQ-DEA (D.N.J. August 25, 2021).

106. A nationwide class of T-Mobile consumers[57] brought at least six lawsuits against the Company in the United States District Courts for the Northern and Central Districts of California seeking compensation, injunctive and declaratory relief under claims of negligence and

---

[55] The lawsuits bring claims under state specific laws as well including: the Washington State Consumer Protection Act (RCW 19.86.010 et seq.); the Washington Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, et seq; the California Consumer Privacy Act § 1798.150; California's Consumer Legal Remedies Act Cal. Civ. Code § 1750, et seq; the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices; Hawaii Security Breach Notification Act, Haw. Rev. Stat. §§ 487N-1, et seq; Hawaii Unfair Practices and Unfair Competition Act, Haw. Rev. Stat. §§ 480-1, et seq.; Hawaii Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. §§ 481A-3, et seq.; Illinois' Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, et seq.; and New York's General Business Law §§ 349, 350, et seq. Additional claims include invasion of privacy, breach of confidence, and breach of the implied covenant of good faith and fair dealing.

[56] The lawsuits have additional state specific subclasses along with the nationwide class. The lawsuits also allege violations of other state specific laws such as the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1, et seq. and the New Jersey Consumer Security Breach Disclosure Act, N.J. Stat. Ann. § 56:8-163, et seq.

[57] A subclass of California T-Mobile consumers is also identified in the lawsuits.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

implied contract and alleging violations of state-specific laws such as California's Consumer Legal Remedies Act Cal. Civ. Code § 1750, et seq.; the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, et seq; and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. *See, e.g., Lang v. T-Mobile USA, Inc*, No. 3:21-cv-06879-BLF (N.D. Cal. September 3, 2021).

107. Another lawsuit was brought by a nationwide class of T-Mobile consumers against the Company in the United States District Court for the Northern District of Georgia seeking compensation, declaratory, and injunctive relief under claims of common law negligence, negligence per se, invasion of privacy, breach of implied contract, and breach of confidence. *See Vash v. T-Mobile U.S. Inc.*, No. 1:21-cv-03384-SCJ (N.D. Ga. Aug. 19, 2021).

108. A nationwide class of T-Mobile consumers brought a lawsuit against the Company in the United States District Court for the Eastern District of New York[58] seeking compensation, declaratory and injunctive relief under claims of common law negligence, negligence per se, breach of expressed and implied contract, misrepresentation, breach of fiduciary duty, and under New York's General Business Law § 349. *See Metzger v. T-Mobile U.S. Inc.*, No. 2:21-cv-04721-JMA-AYS (E.D.N.Y. Aug. 20, 2021).

109. Another nationwide class of T-Mobile consumers[59] brought a lawsuit against the Company in the United States District Court for the Western District of Oklahoma seeking compensation, declaratory, and injunctive relief under claims of common law negligence, invasion of privacy, breach of confidence, breach of implied contract, breach of fiduciary duty, breach of the covenant of good faith and fair dealing, and under the Oklahoma Consumer Protection Act,

[58] A subclass of New York T-Mobile consumers is also identified in the lawsuit.

[59] A subclass of Oklahoma T-Mobile consumers is also identified in the lawsuit.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Okla. Stat., tit. 15, ch. 20 §§ 751, *et seq* and the Oklahoma Deceptive Trade Practices Act, 78 O.S. §§ 51, et seq. *See Peralta, et al. v. T-Mobile U.S. Inc.*, No. 5:21-cv-00838-HE (W.D. Okla. Aug. 24, 2021).

110. Another nationwide class of T-Mobile consumers[60] brought a lawsuit against the Company in the United States District Court for the Western District of Missouri seeking compensation, injunctive and declaratory relief under claims of negligence, breach of confidence, implied contract, invasion of privacy, breach of fiduciary duty, breach of the covenant of good faith and fair dealing, and alleging violations of the Missouri Merchandising Practices Act Mo. Rev. Stat. § 407.010 *et seq*. *See Hill v. T-Mobile U.S. Inc., No.* 2:21-cv-04164-NKL (W.D. Mo. Aug. 25, 2021).

111. A nationwide class of T-Mobile consumers[61] brought a lawsuit against the Company in the United States District Court for the Southern District of Texas seeking compensation, injunctive and declaratory relief under claims of negligence, breach of implied contract, breach of confidence, invasion of privacy, breach of fiduciary duty, and breach of the covenant of good faith and fair dealing. *See Winkler, et al. v. T-Mobile U.S. Inc.*, No. 7:21-cv-00322 (S.D. Tex. Aug. 26, 2021).

H. T-Mobile's False And Misleading Proxy Statement

112. T-Mobile's 2021 Proxy Statement solicited stockholders to, among other things, elect thirteen directors to terms on the Board including Defendants Sievert, Höttges, Claure, Illek, Kübler, Langheim, Tazi, Westbrook, Wilkens, Holloway, Leroy, Datar and Taylor. The 2021

[60] A subclass of Missouri T-Mobile consumers is also identified in the lawsuit.

[61] A subclass of Texas T-Mobile consumers is also identified in the lawsuit.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Proxy Statement was issued by order of the Board and was signed by Defendants Höttges and Sievert.

113. The 2021 Proxy Statement contains the following statement regarding data privacy and cybersecurity:

> ***T-Mobile is committed to maintaining the trust of our customers, employees, partners, and the public by respecting the personal information entrusted to us and handling it responsibly***. Our Information Security and Privacy Council oversees T-Mobile's privacy and security programs, and our Enterprise Risk and Compliance Committee is responsible for T-Mobile's risk management and compliance activities. ***Our Board of Directors maintains oversight in each of these areas via periodic updates to our Nominating and Corporate Governance Committee and the Board. Our Audit Committee also receives updates as appropriate.***
>
> ***We are committed to responsible data use***, including as defined by the CTIA Consumer Code of Conduct and the Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising. We use a variety of administrative, technical and physical security measures to protect our customers' personal data while it is under our control. We maintain security incident response plans to investigate and remediate incidents involving unauthorized access to personal data, and ***we are constantly evolving our safeguards to respond to new risks.***
>
> ***We equip our employees with the knowledge necessary to carry out proper privacy and security practices.***

114. The 2021 Proxy Statement also states that "[u]nderpinning each of our actions is our ongoing commitment to upholding responsible governance practices that ensure accountability, risk oversight and effective leadership at every level of the Company."

115. The 2021 Proxy Statement contains the following statement regarding risk oversight by the Board:

> **THE BOARD'S ROLE IN RISK OVERSIGHT**
>
> **Selective Delegation of Risk Oversight to Committees**
>
> While the full Board has overall responsibility for risk oversight, the Board has delegated risk oversight responsibility for certain risks to committees of the Board.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

> ***On a regular basis, reports of all committee meetings are presented to the Board, and the Board periodically conducts deep dives on key enterprise risks.***

116. The 2021 Proxy Statement further states as follows concerning the Company's commitment to sound corporate governance principles:

> **T-Mobile Is Committed to Good Corporate Governance**
>
> Our corporate governance practices and policies promote the long-term interests of our stockholders, strengthen the accountability of our Board and management and help build public trust.
>
> Our Board has established a boardroom dynamic that encourages meaningful and robust discussions based on each director's unique and diverse background, resulting in informed decision-making that seeks to maximize stockholder value and promotes stockholder interests. ***Directors exercise thorough oversight of decisions regarding the Company's strategy and outlook***. The Board regularly reviews developments in corporate governance and updates its practices and governance materials as it deems necessary and appropriate.

117. The foregoing statements in the 2021 Proxy Statement were false and misleading and omitted material information. In fact, the Board: (1) failed to implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) failed to implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) failed to take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

118. The wrongful conduct alleged herein has damaged T-Mobile, causing the Company to be subject of an investigation by the FCC, numerous class action lawsuits, and irreparably harming its reputation.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

VI. DERIVATIVE ALLEGATIONS

119. Plaintiff brings this action derivatively for the benefit of T-Mobile to redress injuries suffered, and to be suffered, because of the Individual Defendants' breaches of their fiduciary duties, waste of corporate assets, and violation of Sections 14(a) of the Exchange Act, as well as the aiding and abetting thereof.

120. T-Mobile is named solely as a nominal party in this action. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

121. Plaintiff is and has been at all relevant times, a shareholder of T-Mobile. Plaintiff adequately and fairly represents the interests of T-Mobile in enforcing and prosecuting its rights, and, to that end, has retained competent counsel, experienced in derivative litigation, to prosecute this action.

122. Demand upon the Board to institute this action against the Individual Defendants would be futile and is, thus, excused. The Board is neither disinterested nor independent.

123. As directors of T-Mobile, the Individual Defendants were required to implement and maintain an effective system of internal controls for the Company. However, in direct contravention of that duty, the Individual Defendants failed to implement and maintain internal controls or exercise oversight over the security and safety of customer data stored by the Company despite its centrality to the Company's core business. Likewise, the Individual Defendants failed to implement and maintain an effective system of internal controls or exercise oversight over the reporting of truthful, accurate, and complete information in compliance with the federal securities laws.

124. The Board members are not independent of each other and face a substantial likelihood of liability for non-exculpated breaches of their fiduciary duties to the Company and its

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

stockholders by their participation or acquiescence in the wrongdoing alleged herein, their failure to investigate and take action when timely action could have prevented, or at least minimized, the damage caused to T-Mobile by the misconduct pled herein, and their failure to ensure the Company's implementation and maintenance of an adequate system of internal controls and corporate governance practices and procedures.

A. Demand Upon Defendant Sievert Is Excused

125. Defendant Sievert currently serves as the Company's President and CEO, and before that, Sievert served as COO of T-Mobile for a cumulative period of over seven years. Thus, as the Company admits in its Proxy filings, he is not an independent director. The Company provides Defendant Sievert with his principal occupation from which he receives substantial compensation, including $54,914,014 during fiscal year 2020 alone.

126. Sievert signed the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

127. Sievert will not sue those responsible for the wrongdoing pled herein because doing so would harm him and his investments. Sievert holds 669,379 of the Company's shares. If Sievert acknowledged that he, T-Mobile or others engaged in misconduct, his investment in T-Mobile would be substantially devalued. Further, if Sievert acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as the CEO of the Company, either knew of the wrongdoing or should have known of the wrongdoing.

128. Further, Sievert benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

129. Moreover, Sievert was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Sievert, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

130. Sievert is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Sievert is futile and, thus, excused.

B. Demand Upon Defendant Höttges Is Excused

131. Defendant Höttges serves as the Chairman of the Board of T-Mobile and has served as a T-Mobile director for close to eight years. As the Company admits in its Proxy filings, he is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile.

132. Höttges signed the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

133. If Höttges acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as Chairman of the Board of the

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

134. Further, Höttges benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

135. Höttges was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Höttges, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

136. Höttges further failed to uphold his additional obligations under the Company's Code of Ethics. These obligations include, *inter alia*, adhering to and promoting honest and ethical behavior and ensuring that T-Mobile issued complete, fair, accurate, and timely disclosures in its public filings and statements and complied with all applicable laws and regulations.

137. Höttges is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Höttges is futile and, thus, excused.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

C. Demand Upon Defendant Claure Is Excused

138. According to the 2021 Proxy Statement,[62] Claure Mobile LLC ("Claure Mobile"), a Delaware limited liability company wholly owned by Defendant Claure, owns 5,000,000 shares of the Company's common stock. The purchase of these shares was the result of a Master Framework Agreement which the 2021 Proxy Statement describes, in relevant part, as follows:

> On June 22, 2020, the Company entered into a Master Framework Agreement (the "Master Framework Agreement"), by and among the Company, SoftBank, SoftBank Group Capital Ltd., a private limited company incorporated in England and Wales and a wholly owned subsidiary of SoftBank ("SBGC"), Delaware Project 4 L.L.C., a Delaware limited liability company and a wholly owned subsidiary of SoftBank, Project 6 LLC, Claure Mobile, Deutsche Telekom, and T-Mobile Agent LLC, a Delaware limited liability company and a wholly owned subsidiary of the Company ("T-Mobile Agent").
>
> The Master Framework Agreement and related transactions were entered into to facilitate SoftBank's previously announced decision to monetize a portion of the Company's common stock held by SoftBank. As consideration for the Company's facilitation of the SoftBank Monetization, the Independent Committee of the Board of Directors negotiated benefits for T-Mobile and its stockholders….

139. Claure is the current CEO of Softbank International and the COO of Softbank. Claure also served as a director of Softbank for three years and currently serves as a director on the board of two of Softbanks's subsidiaries, Arm Limited and Brightstar. According to the 2021 Proxy Statement, Softbank holds 8.5% of the Company's common stock.

140. Defendant Claure also holds 2,034,791 shares of the Company's common stock that are pledged to secure a line of credit with an unrelated third-party bank.

---

[62] *See* pg. 2 and pg. 67 n. 3 of the 2021 Proxy Statement. The 5,000,000 shares of common stock held by Claure Mobile, are subject to a voting proxy, pursuant to which Claure Mobile has agreed to vote such shares in the manner directed by Deutsche Telekom.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

141. Thus, as the Company admits in its Proxy filings, Defendant Claure is not an independent director based on his substantial investment in T-Mobile through his company, Claure Mobile LLC, and his connection to SoftBank and Brightstar.[63]

142. Defendant Claure authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

143. If Claure acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a major investor with long-term involvement in the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

144. Further, Claure benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

145. Claure was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Claure, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over

[63] Claure also has a strong connection to Deutsche Telekom, a controlling shareholder of T-Mobile, as delineated above and in a later section.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

146. Claure is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Claure is futile and, thus, excused.

D. Demand Upon Defendant Datar Is Excused

147. Datar will not sue those responsible for the wrongdoing pled herein because doing so would harm him and his investments. Datar holds 35,767 of the Company's shares. If Datar acknowledged that he, T-Mobile or others engaged in misconduct, his investment in T-Mobile would be substantially devalued. Further, Datar has served as a director of T-Mobile for close to eight years and receives substantial compensation in the form of fees, stock awards, and other compensation based on his service as a director, including $759,183 during fiscal year 2020 alone.

148. If Datar acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a major investor with long-term involvement in the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

149. Defendant Datar authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

150. Further, Datar benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

151. As Chair of the Audit Committee, Datar had an obligation to protect the Company from substantial risks through the risk assessment and risk management practices described in the Audit Committee Charter. In complete disregard of his obligations under the Audit Committee Charter, Datar failed to ensure that an adequate system of internal controls were implemented and maintained, exposing the Company to cyberattacks to the detriment of T-Mobile, its customers, and stockholders.

152. Moreover, Datar was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Datar, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

153. Datar is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Datar is futile and, thus, excused.

E. Demand Upon Defendant Long Is Excused

154. Defendant Long serves as the Company's National Security Director and has over four decades of experience in security and intelligence. Based on Long's extensive experience, Long was aware or should have been aware that of the severe and imminent danger of cyberattacks

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

on T-Mobile, based on its position as a communications carrier and its reliance on third-party service providers.

155. Moreover, Long was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Long, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

156. Further, Long failed to uphold her additional obligations as a member of the Nominating and Corporate Governance Committee, which include, *inter alia*, ensuring the implementation and effectiveness of the Company's Code of Conduct, compliance and ethics program, and Corporate Governance Guidelines, and annually reviewing the efficacy of the Board.

157. Long is not independent and faces a substantial likelihood of liability for her breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Long is futile and, thus, excused.

F. Demand Upon Defendant Taylor Is Excused

158. Taylor will not sue those responsible for the wrongdoing pled herein because doing so would harm her and her investments. Taylor holds 28,222 of the Company's shares. Defendant Taylor has served as a T-Mobile director for close to eight years and receives substantial

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

compensation in the form of fees, stock awards, and other compensation based on her service as a director, including $767,575 during fiscal year 2020 alone. If Taylor acknowledged that she, T-Mobile or others engaged in misconduct, her investment in T-Mobile would be substantially devalued and her lucrative position jeopardized.

159. If Taylor acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, she would be acknowledging that she, as a major investor with long-term involvement in the Company, either knew of the wrongdoing or should have known of the wrongdoing, which she would not do.

160. Taylor also authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

161. Further, Taylor benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing her re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

162. As a member of the Audit Committee, Taylor had an additional obligation to protect the Company from material risks through the risk assessment and risk management practices described in the Audit Committee Charter. In complete disregard of her obligations under the Audit Committee Charter, Taylor failed to ensure that an adequate system of internal controls were implemented and maintained, exposing the Company to cyberattacks to the detriment of T-Mobile, its customers, and stockholders.

163. Taylor failed to uphold her additional obligations as Chair of the Nominating and Corporate Governance Committee, which include, *inter alia*, ensuring the implementation and

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

effectiveness of the Company's Code of Conduct, compliance and ethics program, and Corporate Governance Guidelines, and annually reviewing the efficacy of the Board.

164. Taylor is not independent and faces a substantial likelihood of liability for her breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Taylor is futile and, thus, excused.

G. Demand Upon Defendant Westbrook Is Excused

165. Westbrook authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

166. Westbrook will not sue those responsible for the wrongdoing pled herein because doing so would harm him and his investments. Westbrook holds 27,692 of the Company's shares. Defendant Westbrook has served as a director of T-Mobile for close to eight years and receives substantial compensation in the form of fees, stock awards, and other compensation based on his service as a director, including $735,899 during fiscal year 2020 alone. If Westbrook acknowledged that he, T-Mobile or others engaged in misconduct, his investment in T-Mobile would be substantially devalued and his lucrative position jeopardized.

167. If Westbrook acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a major investor with long-term involvement in the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

168. Further, Westbrook benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

169. Westbrook was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Westbrook, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

170. As a member of the Audit Committee, Westbrook had an additional obligation to protect the Company from any major financial risks through the risk assessment and risk management practices described in the Audit Committee Charter. In complete disregard of his obligations under the Audit Committee Charter, Westbrook failed to ensure that an adequate system of internal controls were implemented and maintained, exposing the Company to cyberattacks to the detriment of T-Mobile, its customers, and stockholders.

171. Westbrook is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Westbrook is futile and, thus, excused.

H. Demand Upon Defendant Holloway Is Excused

172. Holloway benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing her election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

173. Holloway was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Holloway, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

174. Holloway is not independent and faces a substantial likelihood of liability for her breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Holloway is futile and, thus, excused.

I. Demand Upon Defendant Illek Is Excused

175. Defendant Illek has served as a T-Mobile director for over three years and as the Company admits in its Proxy filings, he is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile. Illek authorized the issuance of the 2021 Proxy Statement despite the false and misleading statements and material omissions it contained.

176. If Illek acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

177. Further, Illek benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

178. Illek was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Illek, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

179. Illek is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Illek is futile and, thus, excused.

J. Demand Upon Defendant Kübler Is Excused

180. Defendant Kübler has served as a T-Mobile director for close to eight years. As the Company admits in its Proxy filings, he is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile.

181. Kübler authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

182. If Kübler acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

183. Further, Kübler benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

184. Kübler was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Kübler, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

185. Kübler is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Kübler is futile and, thus, excused.

K. Demand Upon Defendant Langheim Is Excused

186. Defendant Langheim has served as a T-Mobile director for close to eight years. As the Company admits in its Proxy filings, he is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

187. Langheim authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

188. If Langheim acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

189. Further, Langheim benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

190. Langheim was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Langheim, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

191. Langheim is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Langheim is futile and, thus, excused.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

L. Demand Upon Defendant Leroy Is Excused

192. As the Company admits in its Proxy filings, Defendant Leroy is not an independent director based on her position at Deutsche Telekom, a controlling stockholder of T-Mobile.

193. Defendant Leroy authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

194. If Leroy acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, she would be acknowledging that she, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which she would not do.

195. Further, Leroy benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing her re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

196. Leroy was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Leroy, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

197. Leroy failed to uphold her additional obligations as a member of the Nominating and Corporate Governance Committee, which include, *inter alia*, ensuring the implementation and effectiveness of the Company's Code of Conduct, compliance and ethics program, and Corporate Governance Guidelines, and annually reviewing the efficacy of the Board.

198. Defendants Leroy and Wilkens have long-standing business relationships which preclude them from acting independently and in the shareholders' and Company's best interests. For example, Defendants Leroy and Wilkens serve together as members of the board of directors of Hellenic. Notably, Deutsche Telekom is the largest shareholder of Hellenic since January of 2009. Defendant Wilkens also serves on the board of directors of T-Mobile Netherlands BV, a subsidiary of Deutsche Telekom, and Defendant Langheim serves as the Chairman of the Board of T-Mobile Netherlands BV.

199. Leroy is not independent and faces a substantial likelihood of liability for her breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Leroy is futile and, thus, excused.

M. Demand Upon Defendant Tazi Is Excused

200. As the Company admits in its Proxy filings, Defendant Tazi is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile.

201. Defendant Tazi authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

202. If Tazi acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

203. Further, Tazi benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

204. Tazi was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Tazi, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

205. Tazi is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Tazi is futile and, thus, excused.

N. Demand Upon Defendant Wilkens Is Excused

206. As the Company admits in its Proxy filings, Defendant Wilkens is not an independent director based on his position at Deutsche Telekom, a controlling stockholder of T-Mobile.

207. Defendant Wilkens authorized the issuance of the 2021 Proxy Statement containing false and misleading statements and material omissions and faces a substantial likelihood of liability therefor.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

208. If Wilkens acknowledged that executives at T-Mobile had engaged in the wrongdoing alleged, he would be acknowledging that he, as a director of the Company, either knew of the wrongdoing or should have known of the wrongdoing, which he would not do.

209. Further, Wilkens benefitted from the violation of Section 14(a) of the Exchange Act pled herein by securing his re-election to the T-Mobile Board through the false and misleading statements and material omissions in the 2021 Proxy Statement.

210. Wilkens was aware that data security was material to T-Mobile's core operations but failed to properly oversee this critical aspect of the Company's business. Wilkens, among other things, failed to: (1) implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

211. Defendants Wilkens and Leroy have long-standing business relationships which preclude them from acting independently and in the shareholders' and Company's best interests. For example, Defendants Leroy and Wilkens serve together as members of the board of directors of Hellenic. Notably, Deutsche Telekom is the largest shareholder of Hellenic since January of 2009. Defendant Wilkens also serves on the board of directors of T-Mobile Netherlands BV, a subsidiary of Deutsche Telekom, and Defendant Langheim serves as the Chairman of the Board of T-Mobile Netherlands BV.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

212. Wilkens is not independent and faces a substantial likelihood of liability for his breaches of fiduciary duty and violations of federal securities laws. Any demand upon Defendant Wilkens is futile and, thus, excused.

O. Demand Upon The Deutsche Telekom Defendants Is Excused

213. Half of the Individual Defendants (Höttges, Illek, Kübler, Langheim, Leroy, Tazi, and Wilkens) are directors, executives or officers[64] at Deutsche Telekom, T-Mobile's controlling stockholder (the "Deutsche Telekom Defendants").

214. According to the 2021 Proxy Statement, as of March 31, 2021, Deutsche Telekom has voting control over approximately 52% of the outstanding T-Mobile common stock, including approximately 0.4% of the outstanding T-Mobile common stock held by Claure Mobile. Based on this control, T-Mobile is considered a controlled company under the NASDAQ Stock Market LLC ("NASDAQ") rules. The 2021 Proxy Statement discusses how this level of control affects the Company:

> These rules exempt "controlled companies," like us, from certain corporate governance requirements, including: (i) that a majority of our Board be independent, (ii) that our Nominating and Corporate Governance Committee be composed entirely of independent directors, and (iii) that our Compensation Committee be composed entirely of independent directors. In addition, we rely on the exemption for controlled companies from NASDAQ rules adopted pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act that relate to compensation committee consultants.

[64] Defendant Leroy is a current board member; Defendant Langheim is the current head of the USA & Group Development of Deutsche Telekom; Defendant Illek is the current CFO and member of the board; Defendant Tazi is the current senior VP of Group Innovation and Products; Defendant Kübler is the current senior VP of Corporate Operating Office of Deutsche Telekom; Defendant Höttges is the current Chairman of the Board and CEO of Deutsche Telekom; and Defendant Wilkens is the current senior VP of Group Controlling of Deutsche Telekom.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

215. Deutsche Telekom has the right to appoint ten of the T-Mobile directors and the Deutsche Telekom Defendants were thus appointed to the Board by Deutsche Telekom.[65]

216. Based on the financial and personal connection between each other and Deutsche Telekom, the Deutsche Telecom Defendants would not want to jeopardize Deutsche Telekom's significant financial interest in T-Mobile and their own positions as directors by pursuing litigation against their fellow board members. Therefore, any demand upon the Deutsche Telekom Defendants is futile and excused.

P. Other Factors Demonstrating That Demand Upon The Individual Defendants Is Excused

217. T-Mobile has been and will continue to be exposed to significant losses due to the Individual Defendants' wrongdoing. Yet, the members of the Board have not filed any lawsuits or taken any action against those responsible for the wrongful conduct.

218. The Board knew that T-Mobile was a prime target for cyber-attacks and that the Company had a history of data breaches. The Board was required to investigate and take action to prevent damage to T-Mobile, its shareholders, and customers, but failed to take timely action, ignoring all of the red flags. Had the Board taken timely action the damage caused to T-Mobile could have been prevented or minimized. Thus, demand upon the Board would be futile and is excused.

219. The members of the Board received, and continue to receive, substantial salaries, bonuses, payments, benefits, and other emoluments by virtue of their membership on the Board. They have thus benefited from the wrongs herein alleged and have engaged therein to preserve

[65] Defendant Claure was also designated as a director by Deutsche Telekom and has a strong connection to the Company through the "Master Framework Agreement," as previously delineated.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

their positions of control and the perquisites thereof and are incapable of exercising independent objective judgment in deciding whether to bring this action.

220. Upon information and belief, T-Mobile has Directors & Officers Liability Insurance ("D&O Insurance") policies that contain provisions that would eliminate coverage for any action brought by the Individual Defendants against each other, known as the "insured versus insured exclusion."

VII. CLAIMS FOR RELIEF

FIRST CLAIM
Against the Individual Defendants for Violations of Section 14(a) of the Exchange Act

221. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

222. The Section 14(a) Exchange Act claims alleged herein are based solely on negligence. They are not based on any allegation of reckless or knowing conduct by or on behalf of the Individual Defendants. Plaintiff specifically disclaims any allegations of reliance upon any allegation of, or reference to any allegation of fraud, scienter, or recklessness with regard to the Section 14(a) nonfraud claims.

223. Section 14(a) of the Exchange Act, 15 U.S.C. § 78n(a)(1), provides that "[i]t shall be unlawful for any person, by use of the mails or by any means or instrumentality of interstate commerce or of any facility of a national securities exchange or otherwise, in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors, to solicit or to permit the use of his name to solicit any proxy or consent or authorization in respect of any security (other than an exempted security) registered pursuant to section 12 of this title [15 U.S.C. § 78l]."

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

224. Rule 14a-9, promulgated pursuant to § 14(a) of the Exchange Act, provides that no proxy statement shall contain "any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading." 17 C.F.R. §240.14a-9.

225. Under the direction and watch of the Individual Defendants, the 2021 Proxy Statement failed to disclose, that the Directors each violated their fiduciary duties to T-Mobile and its stockholders by, among other things: (1) failing to implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its customers is safe and secure, as represented; (2) failing to implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) failing to take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

226. Further, the Proxy Statement contained the false and misleading statements related to risk oversight by the Board and the Company's commitment to strong corporate governance principles. The 2021 Proxy Statement also falsely claimed that the Company was actively engaged in training employees in cyber security, constantly evolving to protect customers' private information, and committed to responsible data use and storage.

227. In the exercise of reasonable care, the Individual Defendants should have known that by misrepresenting or failing to disclose the foregoing material facts, the statements contained in the 2021 Proxy Statement were materially false and misleading. These misrepresentations and

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

omissions were material to Plaintiff in voting on the matters set forth for shareholder determination in the Proxy Statement, including, but not limited to the election of directors and ratification of an independent auditor.

228. The false and misleading statements and material omissions in the Proxy Statement led to the re-election of many of the Individual Defendants,[66] which allowed them to continue breaching their fiduciary duties to T-Mobile.

229. The Company was damaged as a result of the Individual Defendants' material misrepresentations and omissions in the Proxy Statement.

230. Plaintiff on behalf of T-Mobile has no adequate remedy at law.

SECOND CLAIM
Against the Individual Defendants for Breach of Fiduciary Duty

231. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

232. Each Individual Defendant owed to the Company the duty to exercise good faith, loyalty, candor and due care in the management and administration of T-Mobile's business and affairs. The Board also had specific duties as defined by the Company's corporate governance documents and principles that, had they been discharged in accordance with the Board's obligations, would have prevented, or at least minimized, the misconduct and consequential harm to T-Mobile alleged herein.

233. The Individual Defendants each violated their fiduciary duties to T-Mobile and its stockholders by, among other things: (1) failing to implement and maintain an effective system of internal controls to ensure that data breaches are prevented and that personal information of its

[66] Defendants Höttges, Claure, Illek, Kübler, Langheim, Tazi, Westbrook, Wilkens, Holloway, Leroy, Datar and Taylor were nominated for election in the 2021 Proxy Statement.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

customers is safe and secure, as represented; (2) failing to implement and maintain effective internal controls and corporate governance practices and procedures to monitor the material risks posed to the Company, its stockholders and customers by the storage of customer data and the "target" such information posed to hackers and other malicious actors; and (3) failing to take action when presented with red flags that internal controls over cybersecurity were inadequate and that bugs on the Company's website allowed hackers to access customers' personal information.

234. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, T-Mobile has sustained and continues to sustain significant damages and its reputation has been irreparably damaged.

235. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company. Plaintiff on behalf of T-Mobile has no adequate remedy at law.

THIRD CLAIM

Against the Individual Defendants for Waste of Corporate Assets

236. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

237. As a result of the foregoing, and by failing to properly consider the interests of the Company and its public shareholders, Defendants have subjected T-Mobile to substantial liability, irreparably damaged the Company's reputation, and wasted corporate assets.

238. As a result of the waste of corporate assets, the Individual Defendants are each liable to the Company.

239. Plaintiff on behalf of T-Mobile has no adequate remedy at law.

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

FOURTH CLAIM
Against the Individual Defendants for Aiding and Abetting

240. Plaintiff incorporates by reference and realleges each and every allegation set forth above as if fully set forth herein.

241. The Individual Defendants are each in breach of their fiduciary duties to the Company and have participated in such breaches of fiduciary duties.

242. In committing the wrongful acts pled herein, each of the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct. In addition to pursuing the wrongful conduct that gives rise to their primary liability, the Individual Defendants also aided and abetted, and/or assisted, each other in breaching their respective duties.

243. Because the actions described herein occurred under the Board's supervision and authority, each of the Individual Defendants played a direct, necessary, and substantial part in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

244. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein.

VIII. PRAYER FOR RELIEF

FOR THESE REASONS, Plaintiff demands judgment in the Company's favor against all Individual Defendants as follows:

(a) Declaring that Plaintiff may maintain this action on behalf of T-Mobile, and that Plaintiff is an adequate representative of the Company;

(b) Declaring that the Individual Defendants have breached and/or aided and abetted the breach of their fiduciary duties to T-Mobile;

(c) Declaring that the Individual Defendants violated Section 14(a) of the Exchange Act;

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

(d) Determining and awarding to T-Mobile the damages sustained by it as a result of the violations set forth above from each of the Individual Defendants, jointly and severally, together with pre-judgment and post-judgment interest thereon;

(e) Directing T-Mobile and the Individual Defendants to take all necessary actions to reform and improve its corporate governance practices and procedures and internal control systems to comply with all applicable laws, rules and regulations and to protect T-Mobile and its shareholders from a repeat of the damaging events described herein;

(f) Awarding T-Mobile restitution from Individual Defendants, and each of them;

(g) Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs, and expenses; and

(h) Granting such other and further relief as the Court may deem just and proper under the circumstances.

IX. JURY DEMAND

Plaintiff hereby demands a trial by jury.

//

//

//

//

//

//

//

//

//

WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010

RESPECTFULLY SUBMITTED AND DATED this 29th day of November, 2021

Yanick Law & Dispute Resolution PLLC

By: */s/ Miles A. Yanick*
Miles A. Yanick
701 Fifth Avenue, Suite 3420
Seattle, Washington 98104
Telephone: (206) 455-5924
Email: myanick@yanicklaw.com

David C. Katz (*pro hac vice* pending)
Mark D. Smilow (*pro hac vice* pending)
Joshua M. Rubin (*pro hac vice* pending)
WEISSLAW LLP
305 Broadway, 7th Floor
New York, New York 10007
Telephone: (212) 682-3025
Facsimile: (212) 682-3010
Email: dkatz@weisslawllp.com
msmilow@weisslawllp.com
jrubin@weisslawllp.com

Counsel for Plaintiff

VERIFICATION

I, Harold Litwin, hereby verify that I am a long-term stockholder of T-Mobile USA, Inc. ("T-Mobile" or the "Company"). As such, I was a stockholder at the time of the transactions complained of in the Verified Stockholder Derivative Complaint ("Complaint"). I am ready, willing, and able to pursue this stockholder derivative action on behalf of T-Mobile. I have reviewed the allegations in the Complaint, and as to those allegations of which I have personal knowledge, I know those allegations to be true, accurate and complete. As to those allegations of which I do not have personal knowledge, I rely on my counsel and their investigation, and for that reason I believe them to be true. Having received a copy of the foregoing complaint, and having reviewed it with my counsel, I hereby authorize its filing.

Harold Litwin
Harold Litwin (Oct 21, 2021 13:56 EDT)

Harold Litwin