STATE OF WASHINGTON
KING COUNTY SUPERIOR COURT

STATE OF WASHINGTON, Plaintiff, v. T-MOBILE US, INC., a foreign corporation, and T-MOBILE USA, INC., a Washington registered corporation, Defendants.	NO. COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff, State of Washington, by and through Robert W. Ferguson, Attorney General, and Mina Shahin, Kathleen Box, Gardner Reed, and Bret Finkelstein, Assistant Attorneys General, brings this action against Defendants T-Mobile US, Inc. and T-Mobile USA, Inc. ("T-Mobile" or "Defendants"). Plaintiff alleges that T-Mobile engaged in unfair and deceptive acts or practices in violation of the Washington Consumer Protection Act (CPA), RCW 19.86. Plaintiff alleges the following on information and belief:

I. INTRODUCTION

1.1 T-Mobile is a large well-known telecommunications carrier that offers mobile communication services, among other products and services, to over 119 million customers. T-Mobile's business model requires prospective and current customers to turn over personally identifiable information (PII). T-Mobile knows the value and risk of maintaining and storing a vast amount of perspective, current, and former customer data.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

1.2 In August 2021 ("August Breach"), T-Mobile failed to adequately secure the PII of over 2 million Washington consumers, including many social security numbers (SSNs).

1.3 Prior to the August Breach, T-Mobile made misleading assurances to the public that it would properly safeguard customer data. However, despite its public statements, the August Breach was a direct result of T-Mobile's lack of accountability. T-Mobile failed to adhere to internal cybersecurity policies as well as recognized industry standards. T-Mobile also ignored its own internal reports that warned of the vulnerabilities that eventually led to and exacerbated the August Breach. T-Mobile's failure to adequately implement cybersecurity measures and address known vulnerabilities, as well as its misleading assurances, violated the CPA.

1.4 In addition to failing to secure consumer PII, T-Mobile also failed to provide adequate notice of the breach to certain affected WA consumers in violation of the CPA. The breach notification to current T-Mobile customers left out critical information about the August Breach and downplayed the severity of the August Breach. Without the pertinent information needed to take steps, or realize steps were needed, to protect their information, those consumers were left vulnerable to fraud and identity theft from nefarious actors.

II. PARTIES

2.1 The Plaintiff is the Attorney General of the State of Washington ("State").

2.2 Defendant T-Mobile US, Inc. is a Delaware limited liability company with its principal place of business in Bellevue, Washington.

2.3 Defendant T-Mobile USA, Inc. is a wholly owned subsidiary of T-Mobile US, Inc., with its principal place of business in Bellevue, Washington.

III. JURISDICTION AND VENUE

3.1 Plaintiff files this Complaint under the provisions of the Consumer Protection Act, RCW 19.86. The Attorney General has the authority to commence this action as conferred by RCW 19.86.080 and RCW 19.86.140.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

3.2 This Court has personal jurisdiction over T-Mobile pursuant to RCW 4.28.180, RCW 4.28.185, and RCW 19.86.160 because T-Mobile has engaged in the conduct set forth in this Complaint in King County and elsewhere in the State of Washington.

3.3 Venue is proper in King County pursuant to RCW 4.12.020 and 4.12.025, and Court Rule 82 because T-Mobile resides and transacts business in King County. T-Mobile also engaged in the conduct set forth in this Complaint in King County and elsewhere in the State of Washington.

IV. FACTUAL ALLEGATIONS

4.1 T-Mobile, is a telecommunications company headquartered in Washington, with a customer base of over 119 million. After completing its merger with Sprint Corporation on April 1, 2020, T-Mobile became the second largest wireless carrier in the United States, increasing its customers from around 67.9 to 102.1 million.

A. The Collection and Use of Consumer PII is an Integral Part of T-Mobile's Business Practices

4.2 As an essential part of modern life, most consumers require a cell phone, yet the options for cell phone service providers are limited. Moreover, consumers have little to no choice over what personal information they must provide a cell phone provider to receive service. Consumers do not have control over how T-Mobile secures personal information.

4.3 T-Mobile's business depends, in part, on the collection of its customers' data. The exhaustive amount of customer data T-Mobile collects and manages includes:

- Personally identifying data such as names, addresses, e-mail addresses, phone numbers, government identification numbers, social security numbers, security codes, signatures, dates of birth, payment information (such as credit and debit cards, and bank account numbers), and gender;
- Location data via T-Mobile cell towers that constantly track customer locations;

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

- Information about its customers' use of T-Mobile products, services, and network, including IP addresses, text and data use history, websites and URLs visited, mobile apps installed or used or that interact with customer devices, and other network analytics and Wi-Fi usage data; and
- Data from sources other than the customer, such as shippers, financial institutions, and credit agencies, and through analyzing customer use of its products and services.

4.4 Prior to its merger with T-Mobile, Sprint likewise collected and managed significant personal data. As of August 2020, immediately prior to the merger, this data included:

- Customer name, gender, marital status, age, date of birth, postal address, telephone number, e-mail address, social security number or other government identification number, physical characteristics or description, bank account numbers, credit card numbers, debit card numbers, activities, location information, education history, employment status and history, as well as consumer personal preferences, trends, and behavior; and
- Data "automatically" collected from customers' devices, including customer location, web sites customers visit, IP addresses, applications purchased, applications downloaded, applications used, and when customer phones were on and functioning.

After the merger, this data continued to be stored in legacy Sprint databases maintained by T-Mobile.

4.5 T-Mobile profits from its collection of personal information. Beyond maintaining a customer database to provide services and products, T-Mobile uses data to send targeted ads to market its services and products. T-Mobile also markets products and services for other companies. In addition, T-Mobile uses personal information to conduct research and perform market analysis.

4.6 T-Mobile also profits from its collection of personal information by providing it to third parties, such as advertising networks like Google Ad Manager. This allows third parties to run analytics and serve targeted ads on behalf of T-Mobile and other companies.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.7 In addition to being used and sold for legitimate purposes, consumers' personal information has immense value to bad actors. Bad actors often sell personal information on the dark web, leading to theft of funds from the consumer whose personal information was stolen.

B. The August Breach Affected Millions of Washington Consumers

4.8 In August 2021, T-Mobile exposed the data of more than 79 million consumers, including current, former, and prospective T-Mobile customers. Over 2 million of the impacted consumers were Washingtonians. The data exposed included social security numbers (SSNs), phone numbers, names, physical addresses, unique International Mobile Equipment Identity (IMEI) numbers, and driver's license information.

4.9 Despite the massive impact of the exposure, a lack of adequate security monitoring and alerting left T-Mobile unaware of the breach until an anonymous cybersecurity threat intelligence firm informed T-Mobile that its customer data was posted for sale on the dark web on August [redacted] 2021, by a threat actor. On information and belief, T-Mobile would have remained in the dark even longer without the outside source notifying them of security failure.

4.10 As early as [redacted] T-Mobile [redacted] of the threat actor that breached T-Mobile's security system in August 2021 [redacted]

4.11 In or around [redacted], the same threat actor gained initial access to T-Mobile's networks, [redacted]. The entry point was [redacted]

4.12 From [redacted] through August [redacted] 2021, the threat actor [redacted] After the entry point was established, the threat actor [redacted] without detection [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted]

4.13 The threat actor discovered [redacted] easily guessable username and password. [redacted] The account credentials was for [redacted]

4.14 The threat actor used access to the [redacted]

4.15 On August [redacted], 2021, the threat actor [redacted] On that date, the threat actor successfully [redacted]

4.16 On August [redacted], 2021, through the [redacted], the threat actor accessed the T-Mobile [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.17 From August [redacted], 2021, the threat actor transferred files, containing copies of consumer information [redacted] The files contained customer names, addresses, phone number, date of birth, SSN, and T-Mobile account information.

4.18 Almost immediately after the data was stolen, the personal information of T-Mobile customers appeared on the dark web for sale to the highest bidder. One dark web forum offered to sell T-Mobile customer data consisting of SSNs, dates of birth, and driver licenses for [redacted]

C. T-Mobile Was Aware of the Risk of Cybersecurity Threats

4.19 T-Mobile is no stranger to data breaches and other cybersecurity incidents resulting from inadequate implementation of data security policies and practices.

- In October 2017 an "ethical hacker" and security researcher found an Application Programming Interface (API) vulnerability that could have exposed PII, including customer names, email addresses, and account numbers, just by knowing or guessing a customer's phone number.
- In August 2018, a hacker used a T-Mobile API to gain access to customer data. While T-Mobile detected the hack and shut it down in less than 24 hours, it was reported that approximately 2 million customers were affected, including names, email addresses, encrypted passwords, account numbers, and other billing information.
- In November 2019, hackers manipulated an authenticated API session for their own accounts to return unauthorized data for other, unrelated customer accounts. The data reportedly exposed included customer names, phone numbers, addresses, account information, and rate, plan and calling features.
- In December 2021, a hacker compromised the T-Mobile for Business Account Hub. The hacker obtained multiple sets of employee credentials and a customer email

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

account giving access to "Customer proprietary network information" such as call logs and minutes used.

- In April 2022, hackers used stolen employee credentials to access internal T-Mobile systems that housed operational tools software. The hackers reportedly stole proprietary T-Mobile source code.

4.20 In the Form 10-K filed with the Securities and Exchange Commission in 2020, T-Mobile stated: "We are subject to the threat of unauthorized access or disclosure of Confidential Information by . . . malicious actors . . . that could compromise the confidentiality and integrity of Confidential Information." T-Mobile went on to state that it would "expect to continue to be the target of cyber-attacks, data breaches, or security incidents."

4.21 T-Mobile also admitted that its merger with Sprint created an additional security risk. In its 2020 Form 10-K, T-Mobile also stated that as a result of operating multiple billing systems during the migration "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."

D. The August Breach was the Result of T-Mobile's Failure to Adequately Implement its Cybersecurity Policies and Procedures

4.22 For years prior to the August Breach, T-Mobile inadequately implemented its cyber security policies and procedures. T-Mobile knew of the risks from cyber-attacks and decided to accept the risks rather than adequately implement safeguards.

4.23 The August Breach threat actor exploited the following known risks to T-Mobile cyber security:

- Inadequate cybersecurity risk management
- Inadequate network configuration management
- Inadequate identification and authentication management
- Inadequate asset management

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

- Inadequate security monitoring and alerting management

4.24 T-Mobile's failure to remediate its cybersecurity vulnerabilities went against its internal policies and procedures, as well as known industry standards. T-Mobile's business practices led directly to the exposure and exfiltration of PII in the August Breach.

1. Cybersecurity Risk Management

4.25 T-Mobile had an inadequate process to conduct security impact assessments for major network changes and potential cybersecurity risks. This significant gap in oversight was a direct contributor to the August Breach, highlighting T-Mobile's failure to implement a cohesive and effective risk management strategy to address vulnerabilities and safeguard against future security incidents.

4.26 [redacted] these deficiencies were rooted in the absence of a comprehensive risk management structure. [redacted] T-Mobile was aware that its risk assessment processes were insufficient for identifying and addressing known security vulnerabilities. [redacted]

4.27 T-Mobile lacked centralized ownership for ensuring compliance with risk assessments and remediation. [redacted]

4.28 [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.29 [redacted] This fragmented approach left significant gaps in their security posture.

4.30 [redacted]

4.31 T-Mobile's persistent deficiencies in security risk management, identified through [redacted], underscores a systemic lack of centralized oversight and accountability, which ultimately resulted in the August Breach.

2. Network Configuration Management

a. T-Mobile failed to [redacted]

4.32 T-Mobile's inadequate [redacted] directly contributed to the August Breach, by allowing the threat actor to easily [redacted]

4.33 T-Mobile was aware of its [redacted] prior to the breach and did not fix the problem. T-Mobile did not prioritize the security of its [redacted] which the threat actor was able to exploit.

4.34 [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted] The identified security standards [redacted] were not met at the time of the August Breach.

4.35 [redacted] T-Mobile did not follow its own requirements.

[redacted]

4.37 T-Mobile's failure to adhere to its [redacted] policies allowed the threat actor to [redacted]

b. T-Mobile failed to [redacted]

4.38 T-Mobile [redacted] allowed the connection from the threat actor's IP address.

4.39 [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted] was not in place at the time of the August Breach.

4.40 [redacted] a well-known risk factor that can lead to significant security vulnerabilities.

4.41 [redacted]

4.42 [redacted]

4.43 [redacted]

4.44 T-Mobile's inadequate network configuration facilitated the threat actor's connection from its IP address and ability to [redacted]

3. Identification and Authentication Management

4.45 T-Mobile used weak credentials [redacted] This included [redacted]

4.46 The threat actor discovered and used the [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted]

4.47 Moreover, based on information and belief, T-Mobile did not implement any rate-limit to authentication attempts. [redacted]

4.48 T-Mobile's identification and authentication management also deviated from its own security policies.

4.49 First, [redacted]

4.50 Second, [redacted]

4.51 Third, [redacted]

4.52 Last, [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

[redacted]

4.53 T-Mobile did not follow [redacted] policies and procedures. [redacted]

4.54 T-Mobile was aware [redacted]

4.55 T-Mobile was also aware [redacted]

4.56 T-Mobile's inadequate password management failed to adhere to FTC standards. The FTC recommends "maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information."

4.57 T-Mobile's inadequate identification and authentication management [redacted], directly contributing to the August Breach.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4. Asset Management

4.58 [redacted]

4.59 [redacted]

4.60 [redacted]

4.61 [redacted]

4.62 [redacted]

4.63 [redacted]

4.64 The FTC also recommends that "keeping customer information in encrypted files provides better protection in case of theft."

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.65 T-Mobile failed to ensure compliance with its asset management policies and procedures, as well as industry standards, [redacted]

4.66 T-Mobile's failure to implement adequate asset management contributed to the August Breach.

5. Security Monitoring and Alerting Management

a. T-Mobile failed to [redacted]

4.67 T-Mobile failed to [redacted]

4.68 The threat actor [redacted]

4.69 The threat actor [redacted]

4.70 [redacted]

4.71 [redacted]

4.72 The threat actor also [redacted]

4.73 The threat actor [redacted]

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.74 [redacted]

4.75 [redacted]

4.76 [redacted]

4.77 Adequate [redacted] would have made T-Mobile aware of the threat actors unauthorized activity and allowed T-Mobile to stop the malicious activities in a timely manner.

4.78 T-Mobile's inadequate [redacted] increased the impact of the August Breach.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

b. T-Mobile failed to [redacted]

4.79 The threat actor [redacted]

4.80 On information and belief, T-Mobile's monitoring and alerting configuration for external connections to the T-Mobile lab environment either never raised an alert from the repeated connections or any alert was disregarded.

4.81 T-Mobile's monitoring and alerting configuration for external connections also failed to [redacted]

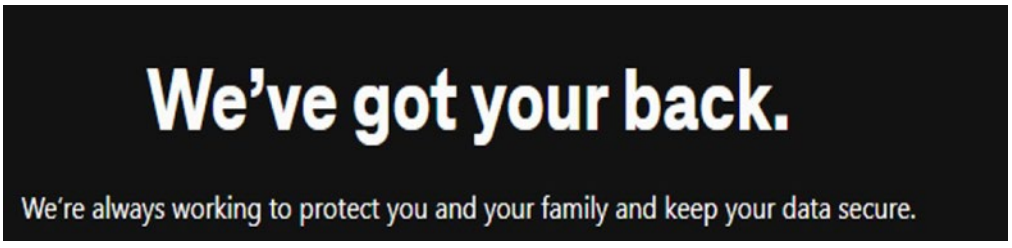
4.82 T-Mobile's inadequate monitoring and alerting configuration facilitated the threat actor's continued access to T-Mobile's network.

E. T-Mobile's Privacy Notices and August Breach Notifications

1. Despite failing to remediate known cybersecurity vulnerabilities, T-Mobile misrepresented that it adequately safeguarded consumer data

4.83 At the time of the August 2021 breach, T-Mobile misrepresented a high level of commitment to protecting customer data. T-Mobile made these statements despite a history of data breaches and cybersecurity incidents in addition to, as explained above, lacking accountability in data security governance.

4.84 At the time of the August Breach, T-Mobile's Privacy Center webpage used bold, prominently featured text that encouraged customers not to worry about the security of their data held by T-Mobile:



ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.85 These statements created a public perception that T-Mobile took care of all its customers' cybersecurity needs, in stark contrast to the ongoing, inadequate implementation of data security policies and practices.

4.86 The "How We Protect Your Data" section of T-Mobile's Privacy Notice webpage as of May 2021 also assured customers their data was safe:

> **How We Protect Your 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.
> Despite our efforts, we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use, or disclose personal data. Be sure to use a strong password to access your information and not one you use for other services. You should also use multi-factor authentication where possible.

4.87 This assurance, however, implies that T-Mobile's security safeguards would prevent all types of unauthorized access attempts apart from customers' own weak passwords. This statement put the onus of maintaining adequate cybersecurity on the consumer and ignored the existence of cybersecurity threats to T-Mobile's networks, such as hackers. Given the lack of adequate cybersecurity efforts as explained above, T-Mobile's statements misrepresented the quality of its data security practices.

4.88 Despite its assurances, T-Mobile failed to implement adequate data security measures to prevent unauthorized access and exposure of consumer PII in the August Breach. T-Mobile's external statements created a public image of a company committed to excellence in cybersecurity in order to protect consumer data despite the reality of T-Mobile's wholly inadequate implementation of basic data security policies and practices, which T-Mobile did not disclose to consumers.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

2. T-Mobile's breach notifications were inadequate

4.89 T-Mobile's data breach notifications to current customers regarding the August Breach were inadequate in a number of ways.

4.90 T-Mobile sent different notifications to different groups of consumers based on whether the consumer was a current or former customer and the type of PII exposed.

4.91 T-Mobile sent breach notifications to current customers by text message. The text messages were brief, omitted critical information, and in certain cases actively misled customers regarding the seriousness of the breach.

4.92 Most critically, T-Mobile failed to notify current customers, whose SSNs were exposed in the August Breach, that their SSN had been exposed. Rather, T-Mobile's notifications to those customers said nothing about SSNs and only informed them that their debit or credit card information was *not* exposed:

> T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here. t-mo.co/Protect

4.93 T-Mobile's decision not to inform customers that their SSNs and other PII had been exposed to criminals on the dark web stands in stark contrast to the choice T-Mobile made when it notified customers whose SSNs were *not* exposed. For those customers, T-Mobile highlighted that their SSNs were not exposed and minimized the perceived impact of the breach:

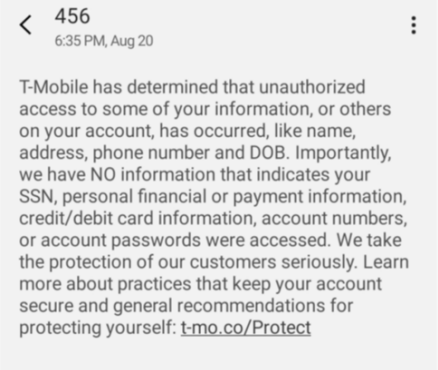
//

//

//

//

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744



4.94 T-Mobile's breach notifications to current customers failed to include the name and contact information of the reporting business, a list of the types of PII exposed in the breach, the time frame of the exposure, or contact information for the major credit reporting agencies. Instead, that required information was only available if the customer chose to click on a link at the end of the notice. That link, however, appeared to relate only to T-Mobile's recommendation that consumers "take action to protect your credit" or to "learn more about practices that keep your account secure and general recommendations for protecting yourself." The text failed to indicate that additional information about the nature of the PII exposed in the breach, or other critical information T-Mobile was required to notify customers about by law, was available at the linked website.

4.95 Furthermore, upon information and belief, T-Mobile's current customers did not consent to receive electronic data breach notifications in the form that T-Mobile provided such notifications of the August Breach, *i.e.*, by text message with a link to T-Mobile's website.

3. T-Mobile's breach notifications misled consumers as to the severity of the August Breach

4.96 Because T-Mobile's breach notifications omitted critical information, T-Mobile's customers were unaware of the seriousness of the August Breach. Instead, customers were left to piecemeal information from various sources to gather all the pertinent information required to take reasonable steps to protect their information.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

4.97 T-Mobile's notifications furthermore failed to inform customers that the breaches may have exposed them to the risk of identity theft and fraud. Indeed, in some instances, customers' PII was available for sale on the dark web after the breaches. If customers had been appropriately notified, they could have taken steps to protect themselves, such as by obtaining credit monitoring, setting up fraud alerts, or getting a security freeze.

4.98 Even into early 2022, thousands of consumers received alerts from McAfee that their information was still on the dark web. Despite this, T-Mobile continued to downplay the severity of the breach. For example, in T-Mobile's 2021 Annual Report to its shareholders, published in February 2022, T-Mobile spent more time reporting what was *not* exposed in the breach rather than elaborating on the vast amount of PII that *was* exposed and remained on the dark web to that day.

V. FIRST CAUSE OF ACTION

(Deceptive Acts in Violation of the Consumer Protection Act, RCW 19.86.020)

5.1 Plaintiff re-alleges Paragraphs 1.1 through 4.98 and incorporates them as if set fully herein.

5.2 T-Mobile engages in "trade" or "commerce" within the meaning of the Consumer Protection Act, RCW 19.86.010(2), when it advertised, offered, and sold goods and services to Washington consumers.

5.3 T-Mobile engaged in deceptive acts or practices within the meaning of RCW 19.86.020 by misrepresenting that it adequately safeguards consumer personal information from unauthorized access or exposure when it misrepresented:

a. The adequacy of its cybersecurity measures;

b. The threat to consumers' data held by T-Mobile; and

c. The scope of the August Breach in its breach notification.

5.4 T-Mobile's conduct had the capacity to deceive a substantial number of Washington consumers.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

5.5 T-Mobile's conduct affects the public interest and is likely to continue without relief from this Court.

5.6 Based on the above deceptive acts and practices, Plaintiff is entitled to relief under the Consumer Protection Act including injunctive relief and restitution pursuant to RCW 19.86.080, civil penalties pursuant to RCW 19.86.140 for each and every violation of RCW 19.86.020, and reimbursement of the costs of this action, including reasonable attorneys' fees, pursuant to RCW 19.86.080.

VI. SECOND CAUSE OF ACTION
(Violation of the Data Breach Notification Statute, Ch. 19.255 RCW, Per Se Violation of the Consumer Protection Act, RCW 19.86.020)

6.1 Plaintiff re-alleges Paragraphs 1.1 through 5.6 and incorporates them as if set fully herein.

6.2 T-Mobile was required to notify consumers of the August Breach pursuant to RCW 19.255.010.

6.3 RCW 19.255.010(4) lists the methods by which T-Mobile could have provided proper notification to consumers: written notice, electronic notice, or substitute notice. T-Mobile's breach notifications to current customers by text message with a link to T-Mobile's website did not comply with the requirements of any of those allowable methods.

6.4 RCW 19.255.010(6) describes the content requirements of the breach notification. Notifications must:

a. List the name and contact information of the reporting business;

b. List the types of PII that are reasonably believed to have been the subject of the breach;

c. Identify the time frame of the exposure, including the date of the breach and the date of the discovery of the breach; and

d. Inform the consumer of the toll-free telephone numbers and addresses of the major credit reporting agencies.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

6.5 T-Mobile's breach notifications to current customers failed to include the name and contact information of the reporting business, a list of the types of PII exposed in the breach, the time frame of the exposure, or contact information for the major credit reporting agencies.

6.6 T-Mobile's violation of Ch. 19.255 RCW is a per se violation of the Consumer Protection Act. RCW 19.255.040(2).

6.7 Based on T-Mobile's violations of Ch. 19.255 RCW, Plaintiff is entitled to relief under the Consumer Protection Act including injunctive relief and restitution pursuant to RCW 19.86.080, civil penalties pursuant to RCW 19.86.140 for each and every violation of RCW 19.86.020, and reimbursement of the costs of this action, including reasonable attorneys' fees, pursuant to RCW 19.86.080.

VII. THIRD CAUSE OF ACTION

(Unfair Acts in Violation of the Consumer Protection Act, RCW 19.86.020)

7.1 Plaintiff re-alleges Paragraphs 1.1 through 6.7 and incorporates them as if set fully herein.

7.2 T-Mobile engages in "trade" or "commerce" within the meaning of the Consumer Protection Act, RCW 19.86.010(2), when it advertised, offered, and sold goods and service to Washington consumers.

7.3 T-Mobile engaged in numerous unfair acts or practices within the meaning of RCW 19.86.020 by, including but not limited to:

a. Failing to implement adequate cybersecurity risk management;

b. Failing to implement adequate network configuration management;

c. Failing to implement adequate identification and authentication management;

d. Failing to implement adequate asset management; and

e. Failing to implement adequate security monitoring and alerting management.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

7.4 T-Mobile's conduct affects the public interest and is likely to continue without relief from this Court.

7.5 Based on the above deceptive acts and practices, Plaintiff is entitled to relief under the Consumer Protection Act including injunctive relief and restitution pursuant to RCW 19.86.080, civil penalties pursuant to RCW 19.86.140 for each and every violation of RCW 19.86.020, and reimbursement of the costs of this action, including reasonable attorneys' fees, pursuant to RCW 19.86.080.

VIII. PRAYER FOR RELIEF

Wherefore, the State prays for the following relief:

8.1 That the Court adjudge and decree that the Defendants have engaged in the conduct complained of herein.

8.2 That the Court adjudge and decree that the conduct complained of constitutes unfair or deceptive acts or practices and is unlawful in violation of the Consumer Protection Act, RCW 19.86.

8.3 That the Court issue a permanent injunction pursuant to the Consumer Protection Act, RCW 19.86.080, enjoining and restraining Defendants and their representatives, successors, assigns, offices, agents, servants, employees, and all other persons acting or claiming to act for, on behalf of, or in concert or participation with Defendants, from continuing or resuming the unlawful conduct complained of herein.

8.4 That the Court assess civil penalties, pursuant to RCW 19.86.140, against Defendants for each and every violation of RCW 19.86.020 caused by the conduct complained of herein.

8.5 That the Court, as an equitable remedy, disgorge Defendants of money or property acquired by Defendants as a result of the conduct and violations complained of herein.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744

8.6 That the Court make such orders pursuant to RCW 19.86.080 as it deems appropriate to provide for restitution to consumers of money or property unlawfully acquired by Defendants as a result of the conduct complained of herein.

8.7 That the Court make such orders pursuant to RCW 19.86.080 to provide that the Plaintiff, State of Washington, have and recover from Defendants the costs of this action, including reasonable attorneys' fees.

8.8 That the Court award prejudgment interest on restitution, if any, awarded in this case.

8.9 For such other relief as the Court may deem just and proper.

DATED this 6th day of January 2025.

ROBERT W. FERGUSON
Attorney General

s/Mina Shahin

MINA SHAHIN, WSBA #46661
KATHLEEN BOX, WSBA #45254
GARDNER REED, WSBA #55630
BRET FINKELSTEIN, WSBA #48845
Assistant Attorneys General
Attorneys for Plaintiff State of Washington
800 Fifth Avenue, Suite 2000
Seattle, WA 98104

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
800 Fifth Avenue, Suite 2000
Seattle, WA 98104-3188
(206) 464-7744