Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
TracFone Wireless, Inc.	)	File Nos.: EB-TCD-22-00033630;
	)	EB-TCD-23-00034682
	)	CD Acct. No.: 202432170006
	)	FRN: 0006855639

ORDER

Adopted: July 19, 2024 **Released: July 22, 2024**

By the Chief, Enforcement Bureau:

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has entered into a Consent Decree resolving the Bureau's investigations into whether TracFone Wireless, Inc. (TracFone or Company): (i) failed to meet its duty to protect the confidentiality of customer proprietary information (PI); (ii) impermissibly used, disclosed, or permitted access to individually identifiable customer proprietary network information (CPNI) without customer approval; (iii) failed to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI; and (iv) engaged in unjust and unreasonable information security practices in connection to three data breaches that occurred between 2021 and 2023. Third-party threat actors gained access to certain TracFone customer information, including PI and CPNI, by exploiting vulnerabilities related to customer-facing TracFone application programming interfaces (APIs). Altogether, the three breaches exposed information for approximately {[ ]}[1] customer accounts. After gaining access to customer information during one of the three breaches, the threat actors completed approximately {[ ]} unauthorized port-outs. The customer information exposed in the data breaches included PI (such as customers' names and billing addresses) and certain CPNI (such as the features customers subscribed to and number of lines on an account).

2. Modern software applications encapsulate an extraordinary amount of complexity in a simplified user interface. Engineers commonly reduce this complexity by splitting an application into smaller components that may only perform a small handful of tasks. An API is the language that these components use to communicate with each other.[2] Unbeknownst to the user, loading a website may require the combined effort of myriad API requests sent between the many components that comprise a website. While APIs greatly improve the modularity and flexibility of software, they dramatically expand the potential attack surface area.[3] Without adequate protection, an attacker may be able to make an API request to any one of these components to perform a malicious action or retrieve private information, including consumer information. The ubiquity of APIs, coupled with their potential proximity to

[1] Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

[2] An API is "a set of software instructions and standards that allows machine to machine communication—like when a website uses a widget to share a link on Twitter or Facebook." Gray Brooks, Gen. Services Admin., *What are APIs?* (Apr. 30, 2012), https://digital.gov/2013/04/30/apis-in-government/. *See* Nat'l Inst. of Standards and Tech., *Application Programming Interface (API)*, https://csrc.nist.gov/glossary/term/application_programming_interface (last visited Apr. 5, 2024) ("A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.").

[3] *See, e.g.*, OWASP, *OWASP API Security Project*, https://owasp.org/www-project-api-security/ (last visited May 15, 2024) (addressing API security and the need to "understand and mitigate the unique vulnerabilities and security risks of" APIs); Cloudflare, *Attack surface grows with the proliferation of APIs,* https://www.cloudflare.com/the-net/api-proliferation/ (last visited May 15, 2024) (citing Gartner Research prediction that "API abuses will move from infrequent to the most-frequent attack vector").

consumer information, make them a common target of attackers and merits increased scrutiny when it comes to security standards.[4]

3. The Communications Act of 1934, as amended (the Act), and the Commission's rules require that carriers take appropriate steps to protect consumers' personal information from unauthorized access, use, or disclosure.[5] Consumers should be able to trust that carriers are living up to such obligations. Thus, the Commission has made clear that it is committed to protecting the personal information of consumers in the United States from misappropriation, breach, and unlawful disclosure, and that it expects telecommunications carriers to take "every reasonable precaution" to protect their customers' proprietary or personal information.[6] That includes reasonable practices as they relate to APIs.

4. The failure to protect the confidentiality of customers' PI violates a carrier's statutory duty under the Act[7] to protect that information. Moreover, impermissibly using, disclosing, or permitting access to individually identifiable CPNI without customer approval and failing to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI violate a carrier's statutory duty under the Act and the requirements of the Commission's CPNI rules, respectively.[8] These failures also constitute an unjust and unreasonable practice in violation of the Act.[9]

5. To settle these matters, TracFone will pay a civil penalty of $16,000,000 and develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into TracFone's business practices to protect consumers against similar data breaches in the future. Specifically, TracFone will be required to improve its privacy and data security practices by: (i) designating a compliance officer with specific knowledge of the information security principles and practices required by the Consent Decree; (ii) implementing a comprehensive information security program that is reasonably designed to protect the security, confidentiality, integrity, and availability of customer information collected, processed, stored, or accessed by TracFone web applications, including APIs; (iii) implementing Subscriber Identity Module (SIM) change and port-out protections; (iv) performing annual assessments of the sufficiency and maturity of the TracFone's information security program; and (vi) providing privacy and security awareness training to employees and certain third-parties.

6. After reviewing the terms of the Consent Decree and evaluating the facts before us, we find that the public interest would be served by adopting the Consent Decree and terminating the referenced investigations regarding TracFone's compliance with sections 201(b), 222(a), and 222(c) of the Act, and section 64.2010(a) of the CPNI rules.

7. In the absence of material new evidence relating to these matters, we do not set for hearing the question of TracFone's basic qualifications to hold or obtain a Commission license or authorization.

---

[4] *See, e.g.*, OWASP, *OWASP API Security Top 10 – 2023*, https://owasp.org/API-Security/editions/2023/en/0x00-header/ (last visited May 15, 2024) (addressing top security risks and mitigation strategies for API security); Ramaswamy Chandramouli, NIST Special Publication 800-204, *Security Strategies for Microservices-based Application Systems* (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204.pdf (providing guidance on "strategies for the secure deployment" of microservices, including their interplay with APIs).

[5] *See* 47 U.S.C. § 222; 47 CFR § 64.2001 *et seq*.

[6] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 n.198 (2007) (citing 47 U.S.C. § 222(a)).

[7] 47 U.S.C. § 222(a).

[8] *See id.* § 222(c); 47 CFR § 64.2010(a).

[9] 47 U.S.C. § 201(b).

8. Accordingly, **IT IS ORDERED** that, pursuant to section 4(i) of the Act, 47 U.S.C. § 154(i), and the authority delegated by sections 0.111 and 0.311 of the Commission's rules, 47 CFR §§ 0.111, 0.311, the attached Consent Decree **IS ADOPTED** and its terms incorporated by reference.

9. **IT IS FURTHER ORDERED** that the above-captioned matters **ARE TERMINATED**.

10. **IT IS FURTHER ORDERED** that a copy of this Order and Consent Decree shall be sent by first class mail and certified mail, return receipt requested, to Harley Raff, Associate General Counsel, Verizon, and David Haga, Associate General Counsel, Verizon, on behalf of TracFone Wireless, Inc., 1300 I Street, NW, Suite 500, Washington, DC, 20005.

FEDERAL COMMUNICATIONS COMMISSION

Loyaan A. Egal
Chief
Enforcement Bureau

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
TracFone Wireless, Inc.	)	File Nos.: EB-TCD-22-00033630;
	)	EB-TCD-23-00034682
	)	CD Acct. No.: 202432170006
	)	FRN: 0006855639
	)	

CONSENT DECREE

1. The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) and TracFone Wireless, Inc. (TracFone or Company), by their authorized representatives, hereby enter into this Consent Decree to resolve the Bureau's investigation into whether TracFone violated sections 201(b) and 222 of the Communications Act of 1934, as amended (Communications Act or Act),[1] and section 64.2010(a) of the Commission's Rules[2] in connection with three Data Incidents described below.

I. DEFINITIONS

2. For the purposes of this Consent Decree, the following definitions shall apply:

(a) "Act" or "Communications Act" means the Communications Act of 1934, as amended.[3]

(b) "Adopting Order" means an order of the Bureau adopting the terms of this Consent Decree without change, addition, deletion, or modification.

(c) "Bureau" means the Enforcement Bureau of the Federal Communications Commission.

(d) "CD Acct No." means account number 202432170006, associated with payment obligations described in paragraph 31 of this Consent Decree.

(e) "Commission" or "FCC" means the Federal Communications Commission and all of its bureaus and offices.

(f) "Compliance Plan" means the compliance obligations, program, and procedures described in this Consent Decree at paragraph 21.

(g) "Covered Data" means:[4]

i. An individual's first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government

[1] *See* 47 U.S.C. §§ 201, 222.

[2] *See* 47 CFR § 64.2010(a).

[3] 47 U.S.C. § 151 et seq.

[4] For the purposes of this Consent Decree, Covered Data does not include information about an individual that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

document used to verify the identity of a specific individual, or other unique identification number used on its own for TracFone authentication purposes;

ii. An individual's username or e-mail address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account;

iii. Unique biometric, genetic, or medical data; or

iv. Other information that is (A) CPNI or (B) certain personally identifiable information – namely social security number and the personally identifiable information in (v).

v. Notwithstanding the above: (A) Dissociated data that, if linked, would constitute personally identifiable information is to be considered personally identifiable if the means to link the dissociated data were accessed in connection with access to the dissociated data; and (B) Any one of the discrete data elements listed in (i) to (iv) of this definition, or any combination of the discrete data elements listed above is personally identifiable information if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.

(h) "Covered Employees" means all employees of TracFone who perform or directly supervise, oversee, or manage the performance of duties involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data, or any duties that relate to the Privacy and Security Requirements.

(i) "Covered Incident" means any instance in which TracFone is required to notify, pursuant to a statutory or regulatory requirement, the Federal Communications Commission that Covered Data was, or is reasonably believed to have been, accessed, acquired, or used by, or disclosed to third parties, without authorization.

(j) "Covered Third Party" means any person or entity that performs services involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data pursuant to a contractual agreement with TracFone or with another Covered Third Party. This definition does not include: (i) network operators that may carry traffic for TracFone as a mobile virtual network operator and that have independent breach reporting obligations and independently are subject to the jurisdiction of the Commission; (ii) retailers that engage in sales activities on behalf of TracFone, but do not access TracFone systems to perform account management functions for TracFone; or (iii) affiliated entities that are wholly owned, directly or indirectly, by Verizon Communications Inc.

(k) "Covered Third Party Employees" means all employees of any Covered Third Party who perform services involving the collection, transmission, processing, access to, use, disclosure, storage, or protection of Covered Data accessible through APIs.

(l) "CPNI Rules" means the Commission Rules set forth at 47 CFR § 64.2001 et seq., and any amendments or additions to those rules subsequent to the Effective Date.

(m) "Customer" means a current, former, or prospective customer of TracFone.

(n) "Customer Proprietary Network Information" or "CPNI" shall have the meaning set forth at 47 U.S.C. § 222(h).

(o) "Data Breach" means when a person, without authorization, or exceeding authorization, gains access to, uses, or discloses Covered Data, except that a breach shall not include a good-faith acquisition of Covered Data by an individual,

employee, agent, partner, or vendor of TracFone where such information is not used improperly or further disclosed.

(p) "Data Incidents" means the instances of unauthorized access to Covered Data that TracFone initially reported to the CPNI Data Breach Portal on or about, January 14, 2022 (Reference Number 2022-194), and January 13, 2023, (Reference Numbers 2023-230 and 2023-245) and were subsequently assigned FCC file numbers EB-TCD-22-00033630, and EB-TCD-23-00034682, respectively.

(q) "Effective Date" means the date when this Consent Decree is signed by all necessary parties.

(r) "Encrypt," "Encrypted," or "Encryption" means rendering data unreadable or indecipherable using an algorithm commensurate with the sensitivity of the data at issue.

(s) "Independent Compliance Officer" or "ICO" means the officer described in the Transaction Order.

(t) "Investigations" means the investigations commenced by the Bureau in file nos. EB-TCD-22-00033630 and EB-TCD-23-00034682 regarding whether TracFone violated the Privacy and Data Protection Requirements.

(u) "Knowledge-Based Verification" means identity verification methods based on knowledge of private information associated with the claimed identity; this includes authentication via security questions.

(v) "Operating Procedures" means the standard internal operating procedures and compliance policies established by TracFone to implement the Compliance Plan.

(w) "Parties" means TracFone and the Bureau, each of which is a "Party."

(x) "Privacy and Security Requirements" means the requirements of sections 222(a) and 222(c) of the Act, and the CPNI Rules.

(y) "Rules" means the Commission's regulations found in Title 47 of the Code of Federal Regulations.

(z) "Sensitive API Keys" means all identifiers used to identify components of Web Applications with internal or external application programming interfaces (APIs), where disclosure of these identifiers would permit the holder to request information or perform actions intended to be restricted to Web Applications.

(aa) "Security Event" means any activity or occurrence that gives rise to a compromise to the security of Covered Data.

(bb) "TracFone" means TracFone Wireless, Inc., and any predecessor-in-interest, wholly or partially owned subsidiary, and includes but is not limited to, all directors, officers, and employees.

(cc) "Transaction Order" means the Commission's order approving Verizon Communications Inc.'s acquisition of control of TracFone's section 214 authorization subject to certain conditions set forth in *Application of Verizon Communications Inc. and American Movil, S.A.B. de C.V.*, GN Docket 21-112, Memorandum Opinion and Order, 36 FCC Rcd. 16994 (2021).

(dd) "Web Applications" means any TracFone applications accessible from the Internet that (1) are public facing and (2) provide access to Covered Data. "Web Applications" include all user interfaces, APIs, software development kits (SDKs), libraries, and other components used by those applications.

II. BACKGROUND

3. *Legal Framework.* The Act and Commission's Rules govern and limit telecommunications carriers' use and disclosure of certain customer data. Under section 201(b) of the Act, all practices in connection with regulated common carrier communication service must be "just and reasonable,"[5] and any such practice that is unjust or unreasonable "is declared to be unlawful."[6]

4. Through section 222 of the Act, Congress established a framework for governing telecommunications carriers' use and protection of information received or obtained by virtue of providing a telecommunications service.[7] Section 222(a) imposes on telecommunications carriers a general "duty to protect the confidentiality of proprietary information of, and relating to, . . . customers."[8]

5. Section 222(c) establishes specific privacy requirements for "customer proprietary network information" or CPNI, namely information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier" and that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[9]

6. The Commission has adopted the CPNI Rules that implement the privacy requirements of section 222.[10] Section 64.2010 of the CPNI Rules, which the Commission adopted in its 2007 CPNI Order, articulates safeguards that carriers must implement to protect CPNI.[11] Section 64.2010(a) requires carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[12] By focusing section 64.2010(a) on reasonableness, the Commission declined to adopt prescriptive security practices.[13] Instead, it "'allow[ed] carriers to determine what specific measures will best enable them to ensure compliance with the requirement that they remain vigilant in their protection of CPNI."[14]

7. *Factual Background*. TracFone is a telecommunications carrier that provides, among other things, mobile voice and data services to consumers throughout the United States. TracFone offers prepaid plans through multiple brands, such as Straight Talk, Total by Verizon Wireless, and Wal-Mart Family Mobile.[15] TracFone is a wholly owned subsidiary of Verizon Communications Inc., which

[5] 47 U.S.C. § 201(b).

[6] *Id.*

[7] *See id.* § 222.

[8] *Id.* § 222(a).

[9] *Id.* § 222(c), (h)(1)(A).

[10] 47 CFR §§ 64.2001-64.2011.

[11] *See id.* § 64.2010.

[12] *Id.* § 64.2010(a).

[13] *See AT&T Inc*, Notice of Apparent Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1746, para. 8 (2020) (*AT&T Location Data NAL*) (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6945-46, para. 34 (2007) (*2007 CPNI Order*)).

[14] *Id.* at 1746, para.8 (quoting *2007 CPNI Orde*r, 22 FCC Rcd at 6945-46, para. 34). Notwithstanding the absence of prescriptive measures in either the Act or the CPNI Rules, the Commission has stated that it looks, in part, to guidance and best practices from relevant governmental entities in determining the reasonableness of a company's cybersecurity and privacy practices. *Id.* at 1747, para.8, n.35.

[15] In the relevant time period, TracFone operated ten distinct brands: (1) TracFone; (2) Straight Talk; (3) Total Wireless; (4) Page Plus; (5) Net 10; (6) Wal-Mart Family Mobile; (7) Simple Mobile; (8) Go Smart; (9) SafeLink Wireless; and (10) Clearway.

acquired TracFone on November 23, 2021.[16] TracFone offers services to approximately {[ ]}[17] subscribers.[18]

8. Between January 2021 and January 2023, TracFone experienced three data incidents, described below, in which external, third-party threat actors attacked TracFone systems in violation of the law and gained unauthorized access to certain Customer information by exploiting vulnerabilities related to Customer-facing TracFone application programming interfaces (APIs).[19] TracFone identified and self-reported the actions of these third-party threat actors and has cooperated with law enforcement in an attempt to bring those threat actors to justice and prevent harm to Customers. Altogether, the three incidents exposed information for approximately {[ ]} Customer accounts (although a large number of those accounts no longer were active or in service). The information that may have been exposed included Customers' names and billing addresses and certain CPNI, such as the features Customers subscribed to and number of lines on an account.

9. *Cross-Brand Incident*. TracFone self-reported the first incident to the Data Breach Reporting Portal on January 14, 2022 (the Cross-Brand Incident).[20] Based on TracFone's report, the Bureau opened its investigation into the Cross-Brand Incident, issuing Letters of Inquiry[21] and conducting meetings with Company representatives. The Company discovered the Cross-Brand Incident in December 2021, when its oversight and monitoring mechanisms flagged an unusually high number of requests to transfer (or "port out") its Customers' phone numbers to other providers, and it received a corresponding unusually high number of Customer complaints about unauthorized port-outs,[22] though threat actors may have accessed TracFone Customer data as early as January 2021.[23] From January 2021

[16] *See generally* Transaction Order; *Verizon completes TracFone Wireless, Inc. acquisition* (Nov. 23, 2021), https://www.verizon.com/about/news/verizon-completes-tracfone-wireless-inc-acquisition.

[17] This material, set off by double brackets {[ ]}, is confidential and is redacted from the public version of this document.

[18] TracFone Wireless, Inc., *About TracFone Wireless, Inc*., https://www.tracfonewirelessinc.com/en/about-us/ (last visited Mar. 11, 2024).

[19] An API is "a set of software instructions and standards that allows machine to machine communication—like when a website uses a widget to share a link on Twitter or Facebook." Gray Brooks, Gen. Services Admin., *What are APIs?* (Apr. 30, 2013), https://digital.gov/2013/04/30/apis-in-government/. *See* Nat'l Inst. of Standards and Tech., *Application Programming Interface (API)*, https://csrc.nist.gov/glossary/term/application_programming_interface (last visited Apr. 5, 2024) ("A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.").

[20] FBI/USSS CPNI Data Breach Reporting Portal Report 2022-194 (Jan. 14, 2022) (on file in EB-TCD-22-00033630). Telecommunications carriers are required to report CPNI breaches through the online portal at https://www.cpnireporting.gov. *See* 47 CFR § 64.2011(b). The data reported through the FCC portal is collected by the U.S. Secret Service and the Federal Bureau of Investigation.

[21] *See* Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to TracFone (Apr. 19, 2022) (on file in EB-TCD-22-00033630); Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to TracFone (Dec. 15, 2022) (on file in EB-TCD-22-00033630); Second Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to TracFone (Apr. 19, 2023) (on file in EB-TCD-22-00033630).

[22] Response to Letter of Inquiry, from TracFone, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 6, Response to Inquiry 1 (June 3, 2022) (on file in EB-TCD-22-00033630) (LOI Response).

[23] *Id.*

to January 2022, threat actors gained access to Customer accounts containing proprietary information,[24] which included certain CPNI and personally identifiable information.[25] After gaining access to the Customer information, the threat actors completed approximately {[ ]} unauthorized port-outs. TracFone subsequently worked with those Customers to have the port-outs reversed and return their service to TracFone, if that was the Customers' preference.[26]

10. In connection with this incident, threat actors exploited certain vulnerabilities related to authentication and a limited number of APIs. By exploiting those vulnerabilities, threat actors were able to gain unauthorized access to certain Customer information.[27]

11. TracFone informed the Bureau that it took steps to remediate the incident and return all phone lines to the correct Customers (i.e., port-in the Customers who had experienced an unauthorized port-out). In January 2022, the Company activated certain port-out notifications to Customers to ensure that any port-out requests that were received were authorized and intended, and began requiring randomly generated PINs from Customers to secure and validate their accounts in connection with requests to port their number to a non-TracFone brand.[28] TracFone also informed the Bureau that it spent several months investigating, testing, and securing the relevant systems after this attack by the external threat actors and had remediated all vulnerabilities associated with the Cross-Brand Incident in 2022.[29]

12. *Order Website Incidents*. Following the Cross-Brand Incident, TracFone experienced two additional incidents, both related to the Company's order websites (collectively, the Order Website Incidents). TracFone reported these incidents to the Data Breach Reporting Portal on December 20, 2022, and January 13, 2023, respectively.[30] The Bureau opened an investigation and issued Letters of Inquiry to the Company.[31] The Order Website Incidents also involved attacks by external threat actors, which exposed certain Customer information,[32] and included certain CPNI as well as other Customer information.[33]

13. Both incidents involved exploiting a vulnerability that allowed the threat actor to access order information (including certain CPNI and other Customer information) without being properly authenticated. The threat actor(s) used two different methods to exploit the vulnerability (switching to a

[24] *Id.* at 35, Response to Inquiry 5; E-mail from Harley Raff, Associate General Counsel, Verizon, to Shana Yates, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Sept. 2, 2023, 08:37 EDT).

[25] *Id.* at 13, Response to Inquiry 1.

[26] *Id.* at 35, Response to Inquiry 5.

[27] *Id.* at 7, Response to Inquiry 1.

[28] *Id.* at 7-8, Response to Inquiry 1.

[29] I*d.* at 23, Response to Inquiry 2.

[30] FBI/USSS CPNI Data Breach Reporting Portal Report 2022-7262 (Dec. 20, 2022) (on file in EB-TCD-23-00034682); FBI/USSS CPNI Data Breach Reporting Portal Report 2023-245 (Jan. 13, 2023) (on file in EB-TCD-23-00034682).

[31] *See* Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Harley Raff, Counsel, TracFone Wireless, Inc. (Jan. 11, 2023) (on file in EB-TCD-23-00034682) (Order Website LOI); Supplemental Letter of Inquiry from Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Harley Raff, Counsel, TracFone Wireless, Inc. (May 25, 2023) (on file in EB-TCD-23-00034682) (Order Website Supplemental LOI).

[32] Response to Order Website LOI, from Harley Raff, Associate General Counsel, Verizon, to Shana Yates, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, at 11, Response to Inquiry 5 (Feb. 24, 2023) (on file in EB-TCD-00034682) (Order Website LOI Response).

[33] Order Website LOI Response at 12, Response to Inquiry 7.

second method when TracFone successfully blocked the first). TracFone ultimately implemented a long-term fix for the underlying vulnerability by February 2023.

14. To resolve these matters, the Parties negotiated the following terms and conditions of settlement and enter into this Consent Decree as provided below.

III. TERMS OF AGREEMENT

15. **Adopting Order**. The provisions of this Consent Decree shall be incorporated by the Bureau in an Adopting Order.

16. **Jurisdiction**. TracFone agrees that the Bureau has jurisdiction over it and the matters contained in this Consent Decree and has the authority to enter into and adopt this Consent Decree.

17. **Effective Date**. The Parties agree that this Consent Decree shall become effective on the Effective Date as defined herein. As of the Effective Date, the Parties agree that this Consent Decree shall have the same force and effect as any other order of the Commission.

18. **Termination of Investigation**. In express reliance on the covenants and representations in this Consent Decree and to avoid further expenditure of public resources, the Bureau agrees to terminate the Investigations into potential violations of 47 U.S.C. §§ 201(b), 222(a), and 222(c), and the CPNI Rules, including 47 CFR § 64.2010(a). In consideration for the termination of the Investigation, TracFone agrees to the terms, conditions, and procedures contained herein. The Bureau further agrees that, in the absence of new material evidence, it will not use the facts developed in the Investigation through the Effective Date, or the existence of this Consent Decree, to institute any new proceeding on its own motion against TracFone concerning the matters that were the subject of the Investigation, or to set for hearing the question of TracFone's basic qualifications to be a Commission licensee or hold Commission licenses or authorizations based on the matters that were the subject of the Investigation.[34]

19. **Admission**. TracFone admits for the purpose of this Consent Decree and for Commission civil enforcement purposes, and in express reliance on the provisions of paragraph 18 herein, that paragraphs 8-13 contain a true and accurate description of the facts underlying the Investigation. No other admissions are made by TracFone.

20. **Compliance Officer**.

(a) Within thirty (30) days after the Effective Date, TracFone shall designate an employee with the requisite corporate and organizational authority to serve as a Compliance Officer. The Compliance Officer must possess or have access to the appropriate authority, reporting lines, independence, resources, education, qualifications, and experience to discharge the duties set forth below. The Compliance Officer may be replaced by another employee with the requisite corporate and organizational authority should he or she change roles or leave his or her employment during the term of this Decree.

(b) The person designated as the Compliance Officer shall be responsible for developing, implementing, and administering the Compliance Plan and ensuring that TracFone complies with the terms and conditions of the Compliance Plan and the Consent Decree. The Compliance Officer may delegate these duties, as necessary, to others, but shall remain the party responsible for the development, implementation and administration of the Compliance Plan.

(c) In addition to the general knowledge of the Privacy and Security Requirements necessary to discharge their duties under the Consent Decree, the Compliance Officer shall have specific knowledge of the information security principles and practices necessary to implement the information security requirements of the Consent Decree,

[34] *See* 47 CFR § 1.93(b).

and the specific requirements of section 222 of the Act, and the CPNI Rules, before assuming his or her duties.

(d) The Compliance Officer must report at least quarterly to Verizon's Chief Privacy Officer, Chief Compliance Officer, and Chief Information Security Officer on TracFone's efforts during the relevant period to comply with the terms and conditions of this Consent Decree.

21. **Compliance Plan and Manual**.

(a) *Compliance Plan*. TracFone must, within two hundred and ten (210) days after the Effective Date, develop and adopt a Compliance Plan designed to ensure future compliance with the Privacy and Security Requirements and with the terms and conditions of this Consent Decree. TracFone will implement, at minimum, the procedures outlined in Paragraphs 22 through 24 in this Consent Decree.

(b) *Compliance Manual*.

i. The Compliance Officer shall, by February 28, 2025, develop and adopt a Compliance Manual.

ii. The Compliance Manual shall explain the Privacy and Security Requirements and the requirements of this Consent Decree, and set forth the procedures that Covered Employees shall follow to ensure TracFone's compliance with the Privacy and Security Requirements and this Consent Decree.

iii. TracFone shall review the Compliance Manual at least every 12 months and revise it as necessary to ensure that the information set forth therein remains current and accurate.

(c) *Compliance Manual Distribution*.

i. The Compliance Officer shall, by February 28, 2025, make available the Compliance Manual to all Covered Employees.

ii. For any future Covered Employees, the Compliance Officer shall distribute the Compliance Manual within thirty (30) days after such future employee assumes their position or responsibilities.

iii. TracFone will make available to Covered Third Parties with which it directly contracts a Compliance Manual specifically tailored Covered Third Parties (the "Covered Third Party Compliance Manual") by February 28, 2025, and request (or require, where contractually possible) that the Covered Third Parties (i) make the Covered Third Party Compliance Manual available to their employees and/or any other Covered Third Parties with which they contract within thirty (30) days, (ii) confirm that they have made the Covered Third Party Compliance Manual available to the required parties, and (iii) take appropriate available measures to address Covered Third Parties who do not provide such confirmation. TracFone may also make reasonable modifications to the Covered Third Party Compliance Manual in response to requests and feedback from Covered Third Parties. TracFone may have more than one version of the Covered Third Party Compliance Manual, tailored to the particular role a given Covered Third Party may have.

iv. TracFone shall make available any material revisions to the Compliance Manual to all Covered Employees within sixty (60) days of making such revisions.

22. **Information Security Program**.

(a) *General*

i. TracFone must, within two hundred and ten (210) days after the Effective Date, revise its Information Security Program to incorporate the measures described in this Consent Decree. While the revised Information Security Program must be in place within two hundred ten (210) days after the Effective Date, that program may contain specific, forward-looking components and future measures that may not necessarily be implemented by that date but will be adopted within the timeframes as set forth therein and/or below. The Information Security Program must be reasonably designed to protect the security, confidentiality, integrity, and availability of Covered Data collected, processed, stored, or accessed by TracFone Web Applications. TracFone's Information Security Program must be documented and must contain reasonable administrative, technical, and physical safeguards based on:

A. The size of TracFone's Customer base and operations;

B. The nature and scope of TracFone's activities that involve Covered Data; and

C. The sensitivity of the Covered Data collected, processed, stored, or accessed by the Web Applications.

ii. The Information Security Program must be regularly reviewed not less than annually and revised with reasonable promptness as necessary following a Covered Incident.

iii. TracFone must provide a copy of the written Information Security Program and any evaluations thereof or updates thereto to the Compliance Officer and Verizon's Chief Privacy Officer, Chief Compliance Officer, and Chief Information Security Officer.

(b) *Compliance Training Program*

i. TracFone shall, by February 28, 2025, launch a Compliance Training Program that provides Covered Employees with training on safeguarding Covered Data that is specific to their roles and responsibilities, as well as training that covers the applicable terms of this Consent Decree. TracFone must provide the training required under this Paragraph to all Covered Employees within 60 days from the launch of the Compliance Training Program and at least annually every calendar year thereafter. For any future Covered Employees, such training must be provided within sixty (60) days of their start date. TracFone must document Covered Employees' completion and reasonable understanding of such training.

ii. TracFone must make training on safeguarding Covered Data available to Covered Third Party Employees, where permissible by contract. TracFone shall require, where permitted by contract, that Covered Third Party Employees repeat TracFone's training on an annual basis, or a comparable training that has been used or developed by the Covered Third-Party.

(c) *Access Control*

i. Within two hundred and ten (210) days of the Effective Date, as part of its Information Security Program, TracFone must adopt policies, procedures, and controls to manage access to, and use of, all accounts with access to Covered

Data, including, without limitation, Customer accounts, administrator accounts, service accounts, and vendor accounts. Such policies, procedures, and controls must establish reasonable standards for access control, account management, and digital authentication that are consistent with those identified by the National Institute of Standards and Technology (NIST) and the Open Worldwide Application Security Project (OWASP). To the extent NIST or OWASP create new standards applicable to TracFone's operations, TracFone shall revise its policies, procedures, and controls to reflect applicable updates within a reasonable amount of time. TracFone must review these policies, procedures, and controls at least annually and update them as reasonably necessary. At a minimum, these policies, procedures, and controls must require the following:

A. Administrative credentials for systems that store or process Covered Data, including, without limitation, account passwords or private SSH ("Secure Shell") keys, must be Encrypted at rest. Access to these credentials must be secured through a password vault, privileged access management, or an equal or greater security tool that is generally accepted by the security industry.

B. All Customer account access by employees or third-party agents must be secured through an authentication mechanism reasonably designed to verify the identity of that employee or agent. Once authenticated, an employee or agent may be granted access to their account resources, without re-authentication, only for a reasonable period of time.

C. All access by Customers to their own Covered Data must be secured through an authentication mechanism reasonably designed to verify the identity of that Customer or an authorized user on that Customer's account. Once authenticated via Web Applications, a Customer may be granted access to their account resources, without re-authentication, only for a reasonable period of time.

D. Web Application queries will not return Covered Data, including CPNI and credit card information, without first requiring authentication and authorization security measures.

E. Account passwords, tokens, private or symmetric cryptographic keys, or Sensitive API Keys, must be stored securely, in a manner that is at least as secure as what is generally accepted by the security industry.

F. Multifactor authentication methods must be offered as an option for Customer authentication in the context of high-risk transactions. The methods offered must be consistent with standards generally accepted by the security industry.

G. Consistent with generally accepted guidance in the security industry (such as NIST 800-63B 5.1.1.2), TracFone will not prompt Customers to use specific types of information (e.g., "What was the name of your first pet?") when choosing passwords, nor will TracFone permit Customers to store "hints" to recover forgotten passwords.

H. TracFone will not exclusively use Knowledge-Based Verification in the form of security questions for Customer authentication or password-reset purposes.

I. Within two hundred and ten (210) days of the Effective Date, TracFone will cease the practice of assigning enumerable or predictable identification numbers to new orders placed by Customers. TracFone will instead assign identifiers to orders using a generation method(s) that does not allow the identifiers to be predicted.

ii. TracFone must engage in reasonable efforts to identify and change or disable default system credentials both for all existing internal systems that contain Covered Data and for new internal systems that contain Covered Data once that new system is implemented, regardless of the level of permissions associated with such credentials.

(d) *Transport Security and Data Sanitization*

i. TracFone must ensure that all data transmitted to and from a Web Application is securely communicated over an encrypted channel with no known vulnerabilities; for example, a TLS ("Transport Layer Security") session.

ii. TracFone must ensure all Web Application input and output is properly validated, sanitized, and stripped against potential known attack methods. This includes, but is not limited to, the following:

A. Any input data sent to a Web Application must be validated and sanitized to prevent common vulnerabilities, such as SQL injection, cross-site scripting attacks, or command injection.

B. Any output data sent from a Web Application must be appropriately sanitized or encoded for the output context to prevent cross-site scripting attacks or other forms of data injection.

(e) *Logging and Monitoring*

i. TracFone must implement and maintain intrusion-prevention and detection systems, endpoint-protection systems, threat-monitoring systems, or similar technologies, reasonably designed to detect and restrict unauthorized access or connections to, and anomalous activities within, the Web Applications. TracFone must assess the effectiveness of these systems every twelve (12) months to ensure that threats are reasonably detected and addressed.

ii. TracFone must adopt reasonable controls to log, monitor, and analyze all security activities on the Web Applications. Such controls will include risk-based behavioral monitoring.

iii. Following a Covered Incident, TracFone must assess the effectiveness of any systems that may not have functioned as intended during the Covered Incident, and address any shortcomings in these systems that allowed the Covered Incident to take place. TracFone must implement reasonable controls to log, monitor, and analyze all security activities on the Web Applications. Such controls will include risk-based behavioral monitoring.

iv. TracFone must regularly monitor all security activities on the Web Applications and make reasonable efforts to identify Security Events.

v. TracFone must establish and maintain a process to prioritize Security Events based on criticality and prevent unreasonable delay in responding to Security Events.

vi. TracFone must engage in reasonable efforts to deploy, monitor and address the results of security vulnerability management tools on Web Applications, using a risk-based assessment to prioritize remediation or mitigation.

vii. TracFone must adopt reasonable procedures designed to retain logs of events that indicate suspicious, unauthorized use or configuration of systems and applications for a reasonable period of time, not less than twelve months, that is sufficient to detect, respond to, and investigate Covered Incidents.

(e) *Asset Inventory*

i. Consistent with industry-accepted best practices, TracFone must develop and maintain and regularly update an inventory of all known assets owned by TracFone that comprise the Web Applications, including but not limited to all software, APIs and electronic data storage. The asset inventory will, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location; (e) the business need for such asset and its purpose; and (f) the risk criticality level of each asset.

ii. TracFone must update the asset inventory at least annually or whenever there is a material change to the Web Applications.

(g) *Patch and Security Update Management*

i. TracFone must maintain reasonable administrative and technical controls to address the potential impact that security patches and security updates may have on the Web Applications and their supporting infrastructure. TracFone must maintain reasonable patch management solutions.

ii. TracFone must timely schedule and install any security update or security patch, as reasonably necessary, considering, without limitation, the severity of the vulnerability for which the update or patch has been released, the severity of the issue in the context of the Web Applications, the impact on TracFone's ongoing business and network operations, whether the vulnerability is being actively exploited by threat actors, and the risk ratings articulated by the relevant software and application vendors or disseminated by the Cybersecurity & Infrastructure Security Agency (CISA) or other relevant governmental authority.

(h) *Software Development and Vulnerability Management*

i. TracFone must implement, maintain, and document a program reasonably designed to identify, assess, and remediate well-known and reasonably foreseeable security vulnerabilities within the Customer-facing Web Applications. This program must require: (a) a system of manual and automated testing during the Software Development Life Cycle ("SDLC") to continually assess and address vulnerabilities before any Web Application code is released into production; and (b) vulnerability scanning of all systems within the Web Applications at least quarterly and promptly, not to exceed thirty (30) days, following a Covered Incident. Documentation of the program must include what was tested during testing (whether annual, in response to a Covered Incident, or otherwise).

ii. TracFone must rate and rank the criticality of all vulnerabilities revealed as a result of testing and scanning by using the Common Vulnerability Scoring

System or comparable industry-accepted methodology. For each vulnerability rated as critical, TracFone must apply a remediation as soon as practicable.

iii. TracFone must perform continuous Static and Dynamic Security Testing (SAST/DAST) of Web Applications, prioritizing APIs, using automated tools that test for vulnerabilities.

iv. The program required by Paragraph i must be reasonably designed to integrate the identification, assessment, and remediation of security issues into the software development lifecycle.

v. TracFone must maintain and regularly perform a reasonable suite of unit and integration tests to verify the correctness of the Web Applications' source code. Test failures must be reasonably investigated and addressed as soon as practicable.

A. Future modifications to Web Application source code shall be accompanied by one or more tests that are reasonably designed to assess the modification and verify that the modified Web Application(s) behave as intended. These tests must be sufficiently comprehensive to provide a reasonable degree of confidence that the modified source code behaves as intended under any input, whether expected or unexpected.

B. The tests required by subparagraph A do not need to be performed in the following situations:

1. The modification is necessary to patch a time-sensitive security vulnerability, in which case these tests must be written and conducted as soon as practicable; or

2. The existing code architecture does not accommodate these tests, in which case the relevant software must be rearchitected in order to support these tests, if possible, as soon as practicable but no later than one (1) year of the original modification through the use of mocks, shims, or other industry-accepted design patterns used to facilitate software testing.

vi. The identification, assessment, and remediation required by this section must include the following:

A. Checking for the vulnerabilities listed in the OWASP API Security Top 10 List (or comparable Industry guidance in the event the OWASP API Security Top 10 List is no longer published); and

B. Reviewing all publicly available, Customer-facing APIs supporting Web Applications to ensure all information that may be included in an API response is either necessary to support the intended functionality of the API, or behind authentication protocols.

(i) *Risk Assessments*

i. TracFone must maintain, and regularly review and revise as necessary, a risk-assessment process reasonably designed to identify, assess, and remediate risks to the Web Applications. This will encompass: (1) a formal risk assessment of any substantive changes made to Web Application architecture, including but not

limited to authentication flows; as well as (2) technical vulnerability assessments of existing Web Applications at least annually.

ii. TracFone must implement Verizon's quantitative risk management platform for the assessment and prioritization of risks. Every TracFone Web Application must also have a compliance profile, which must be updated annually to identify non-compliance with Verizon's security policy. Every instance of non-compliance must have a risk mitigation plan and/or be highlighted for review and acceptance criteria.

iii. TracFone will follow Verizon's programs to ensure that appropriate security architecture and software development controls are identified and addressed for all Web Applications.

iv. TracFone must rate and rank the criticality of all vulnerabilities revealed as a result of any risk assessment and prioritize remediation for any vulnerability that threatens the safeguarding or security of any Covered Data collected, processed, stored, or accessed by the Web Applications.

v. TracFone must address known vulnerabilities identified by TracFone's risk assessments. For each identified vulnerability, TracFone must commence remediation planning as set forth in its Information Security Program and apply the remediation as soon as practicable.

23. **Subscriber Identity Module (SIM) Change and Port-Out Protections**

(a) TracFone must use secure methods that are reasonably designed to authenticate a Customer's identity (or, where a real identity is not provided by Customers, TracFone shall authenticate a Customer based on the information provided to it by such Customer) before effectuating a port-out or SIM change request. TracFone must review, at least annually, and update as necessary, its Customer authentication methods to ensure that such methods continue to be secure.

(b) Upon receipt of a port-out or SIM change request, and before executing the request, TracFone must notify the Customer that such a request associated with the Customer's account was made. In doing so, TracFone must use means reasonably designed to reach the Customer associated with the Customer's account, and clear and concise language that provides sufficient information to effectively inform a Customer that a port-out or SIM change request involving the Customer's number was made.

(c) Prior to executing a port-out or SIM change, TracFone employees must successfully complete authentication.

(d) Upon execution of a port-out or SIM change, TracFone must provide the Customer with confirmation of the transaction.

(e) TracFone must offer Customers a number transfer PIN that will be required before processing requests to port the Customer's number.

(f) TracFone must make available for Customers information about account protection measures TracFone offers, including those to prevent SIM change and port-out fraud. TracFone must make this notice (1) clear and concise and (2) easily accessible through the websites for its brands that sell wireless services to Customers.

(g) TracFone must, by February 28, 2025, develop and implement training for Covered Employees to specifically address unauthorized port-out and SIM change attempts and remediation. Training must include, at a minimum, how to identify unauthorized SIM changes and port-out requests, and the appropriate advice to provide to Customers on how best to protect themselves against this type of fraud. Such training must be administered at least annually every calendar year thereafter. For any future Covered Employees, such training must be provided prior to their starting any work related to port-outs, SIM changes, and remediation related to port-outs and SIM changes. TracFone must document Covered Employees' completion and reasonable understanding of such training through the use of a test at the end of the training.

(h) TracFone must document and monitor the number of fraudulent port-outs and SIM changes at least monthly by channel and dealer/reseller.

(i) To the extent pending or future changes in law impose requirements on TracFone that differ from those in this Consent Decree, TracFone will comply with the applicable law.

24. **Forensic Reports**

(a) Following a Covered Incident that has a material, negative impact (including unauthorized access or use of Covered Data, exposure of financial information, SIM swaps, or port-outs) on 10,000 or more Customers, TracFone must obtain or create (internally, or through the use of external third parties) an investigative report memorializing the facts and circumstances of the Covered Incident, including how it occurred, the scope of the compromise, and any security controls that were exploited in its commission ("Forensic Report"). Each Forensic Report must: (1) be prepared by a qualified, objective, professional; and (2) completed within ninety (90) days of discovery of the Covered Incident. To the extent completion of the investigative report within ninety (90) days is not possible despite TracFone's reasonable efforts, TracFone will notify the Bureau and provide an estimate of when the report will be completed.

(b) Nothing in this section shall prevent or excuse TracFone from obtaining a Forensic Report on a Covered Incident that affects fewer than 10,000 Customers, when doing so is reasonably necessary to thoroughly investigate and analyze the Covered Incident.

25. **Annual Assessments**

(a) TracFone must obtain an initial assessment, followed by annual assessments, of the sufficiency and maturity of the Information Security Program ("Annual Assessments"). TracFone will be responsible for all costs associated with the Annual Assessments. Every two years (i.e., biennially), the Annual Assessments required by this Section must be conducted by an independent third-party (the "Third-Party Assessor") that: (1) uses procedures and standards generally aligned to the NIST cybersecurity framework; and (2) conducts an independent review of the Information Security Program. TracFone will retain all documents relevant to each Assessment for three (3) years after completion of such Assessment and will provide a list of the types of documents provided to the Assessor to the Bureau within thirty (30) days of receipt of a written request. For all other years in which TracFone is required to conduct an Annual Assessment, TracFone is permitted to conduct the Annual Assessments with internal TracFone security experts (the "Internal Assessor";

together with the "Third-Party Assessor," the "Assessor"). The results of these Assessments will be shared internally with TracFone and Verizon's leadership teams.

(b) The initial Annual Assessment must be completed within one year of the Effective Date, and each successive Annual Assessment must be completed one year thereafter, for three (3) years after the Effective Date for the Annual Assessments.

(c) The findings of each Annual Assessment (whether performed by the Third-Party assessor or the Internal Assessor) must be documented in an individual report (the "Assessor's Report"). The Assessor's Reports must:

i. Identify the specific cybersecurity administrative, technical, and physical safeguards maintained by TracFone; and

ii. Document the extent to which the identified administrative, technical and physical safeguards are reasonable considering TracFone's size and complexity, the nature and scope of TracFone's activities, and the sensitivity of the Covered Data maintained by TracFone.

(d) In connection with each Annual Assessment, TracFone must:

i. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Annual Assessment, which measures cybersecurity maturity pursuant to the NIST cybersecurity framework, for which there is no reasonable claim of privilege;

ii. Provide or otherwise make available to the Assessor information about the Web Applications and all of TracFone's relevant information technology assets, and visibility to those portions of the Web Applications and information technology assets deemed in scope; and

iii. Disclose all material facts to the Assessor and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (a) determination of whether TracFone has demonstrated an appropriately mature cybersecurity program; or (b) identification of any material gaps or weaknesses in the cybersecurity program.

(e) After completion of each Annual Assessment:

i. Tracfone must provide a copy of the Assessor's Report to the ICO; and

ii. Consistent with the provisions of the Transaction Order, including without limitation clauses (k) and (n) of Appendix C, Section I(3), the ICO then may ask questions directed to either Assessor and request additional information regarding the completed Annual Assessment, which TracFone and/or the Assessor shall provide.

26. **Reporting Noncompliance**.

(a) TracFone shall report any material noncompliance with the terms and conditions of this Consent Decree within thirty (30) calendar days after discovery of such noncompliance. In complex cases that require additional investigation, TracFone may request up to an additional thirty (30) calendar days, which shall not be unreasonably denied, to make such a report of material noncompliance. Such reports shall include a detailed explanation of:

i. Each known instance of material noncompliance;

ii. The steps that TracFone has taken or will take to remedy such material noncompliance;

iii. The schedule on which such remedial action will be taken; and

iv. Steps that TracFone has taken or will take to prevent the recurrence of any such material noncompliance.

(b) All reports of material noncompliance shall be submitted to:

i. the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 45 L Street NE, Washington, DC 20554, with a copy submitted electronically to Shana.Yates@fcc.gov, John.Tran@fcc.gov, Kimbarly.Taylor@fcc.gov, James.Graves@fcc.gov, Lauren.Merk@fcc.gov and EB-TCD-Privacy@fcc.gov; and

ii. the ICO.

(c) To the extent pending or future changes in law impose requirements on TracFone that differ from those in the Consent Decree, TracFone will comply with the applicable law, and such actions will not constitute noncompliance with the Consent Decree.

(d) To the extent any provisions agreed to in this Consent Decree reference current technologies that become outdated or otherwise ill-suited to TracFone's security needs during the term of this Decree, TracFone may present that information to the Bureau and request an exemption (that shall not reasonably be withheld) from compliance with employing such outdated or ill-suited technology during the remaining term of the Decree.

(e) To the extent TracFone merges with or becomes a wholly owned subsidiary of another Verizon entity, the obligations in this Consent Decree will continue to apply only to TracFone's systems and Customers and not those of the merged or owning entity.

27. **Compliance Reports**

(a) TracFone shall file compliance reports with the Commission six (6) months after the Effective Date, twelve (12) months after the Effective Date, and then annually on the anniversary of the Effective Date up through the full term of this Consent Decree, as set forth in paragraph 30 below. Such compliance reports are expected to contain highly sensitive information about TracFone's systems and security measures that, if disclosed, not only could disadvantage TracFone competitively but could provide bad actors with information that could assist in threat activity. Nothing in this Consent Decree shall directly or indirectly in any way whatsoever impair, prejudice, or otherwise adversely affect TracFone's right to submit such compliance reports under a request for confidentiality.

(b) Each Compliance Report shall include a summary of TracFone's efforts during the relevant period to comply with the terms and conditions of this Consent Decree. In addition, each Compliance Report shall include a certification by the Compliance Officer, as an agent of and on behalf of TracFone, stating that the Compliance Officer has personal knowledge that TracFone: (1) has established and implemented the Compliance Plan; and (2) is not aware of any unreported instances of material noncompliance with the terms and conditions of this Consent Decree, including the reporting obligations set forth in paragraph 26 of this Consent Decree.

(c) The Compliance Officer's certification shall be accompanied by a statement explaining the basis for such certification and shall comply with section 1.16 of the Commission's rules, 47 CFR § 1.16, and be subscribed to as true under penalty of perjury in substantially the form set forth therein.

(d) If the Compliance Officer cannot provide the requisite certification(s), the Compliance Officer, as an agent of and on behalf of TracFone, shall provide the Commission with a detailed explanation of the reason(s) why and describe fully: (1) each instance of material noncompliance; (2) the steps that TracFone has taken or will take to remedy such material noncompliance, including the anticipated schedule on which proposed remedial actions will be taken; and (3) the steps that TracFone has taken or will take to prevent the recurrence of any such material noncompliance, including the anticipated schedule on which such preventative action will be taken.

(e) All Compliance Reports shall be submitted to:

i) the Chief, Telecommunications Consumers Division, Enforcement Bureau, Federal Communications Commission, 45 L Street NE, Washington, DC 20554, with a copy submitted electronically to Shana.Yates@fcc.gov, John.Tran@fcc.gov, Kimbarly.Taylor@fcc.gov, James.Graves@fcc.gov, Lauren.Merk@fcc.gov, and EB-TCD-Privacy@fcc.gov; and

ii) the ICO.

28. **Compliance Monitoring**

(a) For matters concerning this Consent Decree, representatives of the Bureau are authorized to communicate directly with TracFone, but only after notice to TracFone's in-house counsel. TracFone must permit representatives of the Bureau to interview anyone affiliated with TracFone, if such individual has agreed to an interview, after being provided with the opportunity to discuss the request with TracFone's in-house counsel. The interviewee may have counsel present.

(b) The Bureau may use all other lawful means, including posing through its representatives as Customers, suppliers, or other individuals or entities, to TracFone or any individual or entity affiliated with TracFone, without the necessity of identification or prior notice. Nothing in this Consent Decree limits the Commission's lawful use of compulsory process pursuant to the Act.

29. **Recordkeeping**. TracFone must create and retain certain records relating to its compliance with this Consent Decree from the Effective Date up through the full term of this Consent Decree, as set forth in paragraph 30 of this Consent Decree, unless otherwise specified below. Specifically, TracFone must create and retain the following records:

(a) For four (4) years after the date of preparation of each Annual Assessment required by paragraph 25 this Consent Decree, TracFone must retain all materials and evidence that the related auditors/assessors considered, reviewed, relied upon or examined to prepare the Annual Assessment, whether prepared by or on behalf of TracFone, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning TracFone's compliance with related provisions of this Consent Decree, for the compliance period covered by such Annual Assessment;

(b) For three (3) years from the date received, TracFone must retain copies of all subpoenas and other communications with law enforcement, if such communications relate to TracFone's compliance with this Consent Decree;

(c) For three (3) years from the date created or received, TracFone must retain all records, whether prepared by or on behalf of TracFone, that tend to show any lack of material compliance by TracFone with this Consent Decree; and

(d) All records necessary to demonstrate full compliance with each provision of this Consent Decree, including all submissions to the Bureau.

30. **Term**. With the exception of paragraphs 22 and 25, the requirements set forth in this Consent Decree shall expire three (3) years after the Effective Date. The requirements set forth in paragraphs 22 and 25 shall expire four (4) years after the Effective Date.

31. **Civil Penalty**. TracFone must pay a civil penalty of $16,000,000 to the United States Treasury within thirty (30) calendar days of the Effective Date. TracFone acknowledges and agrees that upon execution of this Consent Decree, the Civil Penalty shall become a "Claim" or "Debt" as defined in 31 U.S.C. § 3701(b)(1).[35] Upon an Event of Default, all procedures for collection as permitted by law may, at the Commission's discretion, be initiated. TracFone shall send electronic notification of payment to John Tran at John.Tran@fcc.gov, Kimbarly Taylor at Kimbarly.Taylor@fcc.gov, and EB-TCD-Privacy@fcc.gov on the date said payment is made. Payment of the Civil Penalty must be made by credit card using the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts Civil Penalty payments by check or money order. Below are instructions that payors should follow based on the form of payment selected: [36]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[37] or printed CORES form[38] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[39] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The

[35] Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321, 1358 (Apr. 26, 1996).

[36] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6).

[37] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[38] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[39] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.

- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the CD Acct. No. The bill number is the CD Acct. No. with the first two digits excluded (e.g., CD 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

32. **Event of Default**. TracFone agrees that an Event of Default shall occur upon the failure by TracFone to pay the full amount set forth in paragraph 31 on or before the due date specified in this Consent Decree.

33. **Interest, Charges for Collection, and Acceleration of Maturity Date**. After an Event of Default has occurred under this Consent Decree, the then unpaid amount of the Civil Penalty shall accrue interest, computed using the U.S. Prime Rate in effect on the date of the Event of Default plus 4.75%, from the date of the Event of Default until payment in full. Upon an Event of Default, the then unpaid amount of the Civil Penalty, together with interest, any penalties permitted and/or required by the law, including but not limited to 31 U.S.C. § 3717 and administrative charges, plus the costs of collection, litigation, and attorneys' fees, shall become immediately due and payable, without notice, presentment, demand, protest, or notice of protest of any kind, all of which are waived by TracFone.

34. **Waivers**. As of the Effective Date, TracFone waives any and all rights it may have to seek administrative or judicial reconsideration, review, appeal or stay, or to otherwise challenge or contest the validity of this Consent Decree and the Adopting Order. TracFone shall retain the right to challenge Commission interpretation of the Consent Decree or any terms contained herein. If either Party (or the United States on behalf of the Commission) brings a judicial action to enforce the terms of the Consent Decree or the Adopting Order, neither TracFone nor the Commission shall contest the validity of the Consent Decree or the Adopting Order, and TracFone shall waive any statutory right to a trial *de novo*. TracFone hereby agrees to waive any claims it may otherwise have under the Equal Access to Justice Act[40] relating to the matters addressed in this Consent Decree.

35. **Severability**. The Parties agree that if any of the provisions of the Consent Decree shall be held unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire Consent Decree, but rather the entire Consent Decree shall be construed as if not containing the particular unenforceable provision or provisions, and the rights and obligations of the Parties shall be construed and enforced accordingly.

36. **Invalidity**. In the event that this Consent Decree in its entirety is rendered invalid by any court of competent jurisdiction, it shall become null and void and may not be used in any manner in any legal proceeding.

37. **Subsequent Rule or Order**. The Parties agree that if any provision of the Consent Decree conflicts with any subsequent Rule or order adopted by the Commission (except an order specifically intended to revise the terms of this Consent Decree to which TracFone does not expressly

[40] *See* 5 U.S.C. § 504; 47 CFR §§ 1.1501-1.1530.

consent) that provision will be superseded by such Rule or order.

38. **Savings Clause**. Nothing in this Consent Decree alters or supersedes the terms and conditions of the Transaction Order including, without limitation, clauses (b), (e), (f), (j), (k) and (n) of Appendix C, Section I(3). By signing this Consent Decree, the Company does not waive any arguments with regard to whether or how the terms or conditions of the Transaction Order may apply to any other matter.

39. **Successors and Assigns**. TracFone agrees that the provisions of this Consent Decree shall be binding on its successors, assigns, and transferees.

40. **Final Settlement**. The Parties agree and acknowledge that this Consent Decree shall constitute a final settlement between the Parties with respect to the Investigations.

41. **Modifications**. This Consent Decree cannot be modified without the advance written consent of both Parties.

42. **Paragraph Headings**. The headings of the paragraphs in this Consent Decree are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Decree.

43. **Authorized Representative**. Each Party represents and warrants to the other that it has full power and authority to enter into this Consent Decree. Each person signing this Consent Decree on behalf of a Party hereby represents that he or she is fully authorized by the Party to execute this Consent Decree and to bind the Party to its terms and conditions.

44. **Counterparts**. This Consent Decree may be signed in counterpart (including electronically or by facsimile). Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

_____
Loyaan A. Egal
Chief
Enforcement Bureau

_____
Date

_____
Andrea Short
SVP & Chief Litigation Counsel – Verizon
On Behalf of TracFone Wireless, Inc.

_____
Date