

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of

Verizon Request for Declaratory Ruling,  
or, in the Alternative, for Partial Waiver,  
Regarding the Handset Locking Rule for  
C Block Licensees

WT Docket No. 06-150

To: The Commission

**VERIZON REQUEST FOR DECLARATORY RULING,  
OR, IN THE ALTERNATIVE, FOR PARTIAL WAIVER**

William H. Johnson  
*Of Counsel*

Tamara L. Preiss  
VERIZON  
1300 I Street, N.W.  
Suite 500 East  
Washington, D.C. 20005  
(202) 515-2540

Evan Leo  
Sami M. Ahmed\*  
KELLOGG, HANSEN, TODD, FIGEL  
& FREDERICK, P.L.L.C.  
1615 M Street, N.W.  
Suite 400  
Washington, D.C. 20036  
(202) 326-7930

*\*Not admitted in the District of  
Columbia. Practice supervised by  
members of the firm.*

*Counsel for Verizon*

February 22, 2019

**TABLE OF CONTENTS**

I. INTRODUCTION AND SUMMARY ..... 1

II. BACKGROUND..... 5

III. THE COMMISSION SHOULD DECLARE THAT VERIZON MAY LOCK PHONES TEMPORARILY TO REDUCE FRAUD AND IDENTITY THEFT .. 11

    A. The Commission Should Declare That Temporary Locking of Handsets To Reduce Fraud and Identity Theft Does Not Violate Rule 27.16(e)..... 11

    B. The Commission Should Declare That Temporary Locking of Handsets Does Not Constitute “Configuring” Handsets To Prohibit Use on Other Networks..... 14

    C. These Requested Declaratory Rulings Are Consistent with the Commission’s Open Device Rules ..... 15

IV. IN THE ALTERNATIVE, THE COMISSION SHOULD GRANT A PARTIAL WAIVER OF RULE 27.16(e) TO ALLOW VERIZON TO IMPLEMENT ITS TEMPORARY LOCKING PROPOSAL..... 16

V. CONCLUSION ..... 20

Attachment A: Declaration of Stephen Schwed

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of

Verizon Request for Declaratory Ruling, or,  
in the Alternative, for Partial Waiver,  
Regarding the Handset Locking Rule for  
C Block Licensees

WT Docket No. 06-150

**VERIZON REQUEST FOR DECLARATORY RULING,  
OR, IN THE ALTERNATIVE, FOR PARTIAL WAIVER**

Pursuant to Section 1.2 of the Commission’s rules, Verizon<sup>1</sup> requests a declaratory ruling regarding the handset locking rule for C Block licensees. In the alternative, Verizon seeks a partial waiver of this rule pursuant to Section 1.3 of the Commission’s rules.<sup>2</sup> Verizon seeks this relief to better protect its customers and itself from identity theft and related forms of handset fraud — large and growing problems that significantly harm legitimate customers who are the primary victims of these crimes. This relief will protect consumers by enabling Verizon to combat fraud and identity theft more effectively, a result squarely in the public interest.

**I. INTRODUCTION AND SUMMARY**

Verizon currently provides 4G LTE handsets to customers unlocked upon purchase, which means these devices can be used on any carrier’s compatible 4G LTE network, anywhere in the world. Although there are many benefits to unlocking devices — and Verizon fully

---

<sup>1</sup> For purposes of this filing, Verizon includes Cellco Partnership d/b/a Verizon Wireless.

<sup>2</sup> Following discussions with Staff, Verizon is filing this request in the docket in which the Commission adopted the rules concerning the 700 MHz Upper Band C Block because Verizon seeks a declaratory ruling regarding one of those rules and, in the alternative, a partial waiver of that rule. To the extent Verizon’s request implicates 47 C.F.R. § 1.925(b), which requires filing FCC Form 601, Verizon requests a waiver of that requirement.

supports the consumer choice enabled by unlocking — one unfortunate consequence is that it facilitates theft of these devices and may encourage identity theft by bad actors interested in fraudulently obtaining devices. This is because the value of a device on the black market depends, in part, on the ability of that device to be used on any network and anywhere in the world. A rapidly growing form of handset theft involves what the Commission has termed “subscriber fraud,” which is a form of identity theft. Thieves use a stolen identity or other fraudulent means to obtain a new handset on an existing customer’s account or to open a new wireless service account, and then immediately turn around and sell the handset on the black market without ever paying for the device or the service. When this occurs, Verizon typically will not learn about the fraud unless it is reported by the consumer whose identity was stolen or when the bill on the account goes unpaid. There has also been a rise in first-party fraud, which occurs when an individual uses his or her actual identity to acquire new handsets legally but without any intent to pay for them. First-party fraud is often driven by aggregation schemes that orchestrate the fraud across many coordinated participants, who may receive a portion of the stolen proceeds and coaching on how to disclaim the debt.

Identity theft and first-party fraud significantly harm consumers. Victims of identity theft often struggle to show they did not purchase the devices fraudulently linked to their accounts and face challenges reclaiming their identities. Verizon and other wireless carriers must implement increasingly stringent measures to guard against this unlawful behavior, which inconveniences legitimate customers and degrades their experience. When handset fraud occurs, Verizon loses nearly the entire value of each device, which raises the costs of providing service to all consumers.

Every other large U.S. wireless carrier has continued to lock 4G LTE handsets at the time of purchase, at least in part to help prevent this type of fraud and identity theft. Neither Sprint, T-Mobile, nor AT&T provides 4G LTE handsets unlocked at the time of purchase as Verizon does. Rather, they unlock a new handset only when it has been fully paid off, and even then generally only after some period has passed following activation of the device. These practices provide the time necessary to determine if a handset has been obtained through fraud or identity theft, enabling the wireless provider to receive and process an initial payment on the account.

Verizon seeks to adopt a temporary, 60-day lock on the 4G LTE handsets it provides to ensure they are purchased by a bona fide customer. This targeted, 60-day period will enable Verizon to determine whether a new device was obtained by a legitimate customer who makes the first payment on that device and that the payment clears processing. Locking devices on a temporary basis while Verizon determines whether the device is associated with an actual customer will help Verizon reduce theft of these devices by making them less attractive for resale on the black market. Unlike other large U.S. wireless carriers, however, Verizon will unlock the device automatically at the end of the 60-day period, regardless of whether the device has been fully paid off by that time. Thus, even after implementing this targeted approach, Verizon will continue to lead the wireless industry in platform and device openness.

Verizon has not yet taken these steps to protect itself and its customers due to a lack of clarity regarding the Commission's handset locking rule, which applies to the C Block licenses that Verizon uses for 4G LTE services. Rule 27.16(e) provides that no C Block licensee "may disable features on handsets it provides to customers, or . . . configure handsets it provides to prohibit use of such handsets on other providers' networks."<sup>3</sup> The temporary locking that

---

<sup>3</sup> 47 C.F.R. § 27.16(e).

Verizon contemplates, however, would apply only until such time that Verizon can determine that the handset is provided to a legitimate “customer.” Thus, a temporary lock is unlikely to affect a legitimate customer and would not implicate the rule.

The problem arises because Verizon cannot confirm that a handset has been purchased by a legitimate customer until after it receives the first payment on the account and that payment clears processing. In that scenario, the temporary lock Verizon contemplates would not affect individuals that Verizon knows to be actual customers, and would be removed once Verizon had time to make that determination. Nor would these customers suffer any material harm as a result of a temporary lock, because it is exceedingly rare for a legitimate customer to obtain a new handset from Verizon on an existing or new account and then switch providers within the first 60 days. The small fraction of legitimate customers who choose to terminate service within the first 60 days usually do so within the 14-day return period and return their phones to Verizon.

Given these circumstances, it is not clear that the temporary locking Verizon contemplates would affect a legitimate “customer,” and, therefore, whether it implicates Rule 27.16(e) at all. Nor would Verizon’s temporary lock “configure handsets . . . to prohibit use of such handsets on other providers’ networks.” Verizon’s 4G LTE handsets could be used on other providers’ compatible networks upon expiration of the temporary locking period aimed at identifying legitimate customers. This type of temporary locking with a pro-consumer and pro-competitive purpose is not the type of locking with which the C Block rules and order were concerned.<sup>4</sup> Accordingly, Verizon requests the Commission issue a declaratory ruling to remove

---

<sup>4</sup> *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, et al.*, Second Report and Order, 22 FCC Rcd 15289 (2007) (“*Second C Block Order*”); *see infra* pp. 17-19.

this uncertainty and to clarify that Verizon’s proposed temporary locking to identify legitimate customers and weed out fraudulent ones is consistent with the Commission’s rules.

To the extent the Commission declines to issue a declaratory ruling, Verizon asks the Commission to grant a partial waiver of its rules to enable Verizon to take reasonable steps to address identity theft, first-party fraud, and related forms of theft. There is ample good cause to grant this relief. Allowing Verizon to combat this fraud, as other large U.S. wireless providers do, will help deter bad actors that are currently costing Verizon and its customers more than *\$190 million per year*. The attached Declaration of Stephen Schwed details these losses as well as the extensive steps Verizon is already taking to mitigate them.<sup>5</sup> But as most of the industry has already concluded, those measures can only go so far, and temporary handset locking is an effective means to prevent and deter such crime. The requested relief will also help reduce the other negative consumer impacts of handset fraud that are more difficult to quantify, such as increased risk of identity theft and greater inconvenience for actual and prospective customers as well as consumers generally.

## **II. BACKGROUND**

Theft of mobile handsets is a significant and growing problem that harms Verizon and its customers. One rapidly growing form of theft involves what the Commission has labeled “subscriber fraud” — “when someone signs up for service with fraudulently obtained customer information or false identification.”<sup>6</sup> According to data the Commission cited, there were

---

<sup>5</sup> See Attachment A, Declaration of Stephen Schwed (“Schwed Declaration” or “Schwed Decl.”).

<sup>6</sup> FCC, *Cell Phone Fraud* (Sept. 8, 2017), <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. A related form of fraud involves the use of a synthetic identity, where a profile of information is created using credit report practices that allow sharing of credit-history data of a legitimate individual paired with a fictitious name and identity. See Schwed Decl. ¶ 5.

approximately 340,000 victims of fraudulent mobile-phone accounts in 2017, an increase of 63 percent from 2016.<sup>7</sup> When this theft occurs, it often involves a thief using a stolen identity to obtain new handsets, which are then resold on the black market.<sup>8</sup> In addition, there is a great deal of first-party fraud, in which an individual applies for service and a new handset legally, but with the intent of never paying for the device.<sup>9</sup> Such individuals are frequently victims of aggregation schemes that orchestrate the fraud, promising the individual a portion of the stolen proceeds and often coaching them how to disclaim the debt.<sup>10</sup>

Verizon already takes extensive steps to ensure that potential new customers are who they say they are and that they pass a credit check, and Verizon is continuing to invest in new ways to reduce fraud.<sup>11</sup> Verizon uses a wide variety of data, including from outside sources, to identify potential red flags of fraud, such as stolen credit card numbers and suspicious IP

---

<sup>7</sup> Octavio Blanco, *A New Threat to Your Finances: Cell-Phone Account Fraud*, Consumer Reports (June 4, 2018), <https://www.consumerreports.org/scams-fraud/cell-phone-account-fraud> (citing Javelin Strategy and Research, an advisory firm for the financial industry); *see also* Lorrie Cranor, FTC Chief Technologist, *Your Mobile Phone Account Could Be Hijacked by an Identity Thief*, Tech@FTC Blog (June 7, 2016), <https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief> (chronicling the growing problem of mobile phone identity theft).

<sup>8</sup> Mike Perlstein, *The Black Market of Stolen Cellphones: How To Protect Yourself*, WWLTV (May 16, 2017), <https://www.wwltv.com/article/news/investigations/the-black-market-of-stolen-cellphones-how-to-protect-yourself/440335966>. *See* Schwed Decl. ¶ 5.

<sup>9</sup> *See* Schwed Decl. ¶ 5.

<sup>10</sup> *See id.* This is related to “credit muling,” which involves a scammer that recruits targets, known as “mules,” to purchase numerous phones under separate contracts and give them to the scammer for some sort of compensation. The mules do not know that they have been duped until they try to cancel the contracts. At this stage, the mule often defaults, leaving him or her in financial disarray and the carrier with unpaid and uncollectable receivables. *See* Colleen Tressler, Consumer Education Specialist, *Whoa There! Watch Out for Cell Phone “Credit Muling,”* Federal Trade Commission (June 11, 2014), <https://www.consumer.ftc.gov/blog/2014/06/whoa-there-watch-out-cell-phone-credit-muling>.

<sup>11</sup> *See* Schwed Decl. ¶¶ 13-16.



addresses.<sup>12</sup> Verizon also operates a proprietary fraud decision engine that uses known information about an individual to assign a risk score, which may prompt Verizon to seek additional information as part of the authentication process, such as answers to Knowledge-Based Authentication (“KBA”) questions (*e.g.*, the name of the individual’s first pet or mother’s maiden name) or other tools commercially available for fraud risk mitigation.<sup>13</sup> Verizon participates in the GSMA IMEI (International Mobile Equipment Identity) database, a centralized global database through which Verizon reports the IMEI of stolen phones, so that other carriers consulting the database will not activate them, thus helping to deter theft. This deterrent is weak, however, because relatively few foreign carriers participate.<sup>14</sup> As Mr. Schwed explains, all of these fraud prevention measures have limitations in preventing even known forms of identity theft and related frauds, and criminals are constantly devising new strategies and techniques to thwart fraud detection mechanisms.<sup>15</sup>

Handset theft has increased for several reasons. First, the cost of handsets has skyrocketed, with the most popular devices now retailing for \$1000 or more.<sup>16</sup> Second, 4G LTE devices sold in the U.S. are compatible with many 4G LTE networks abroad, whereas in the past

---

<sup>12</sup> *See id.* ¶ 14.

<sup>13</sup> *See id.* ¶¶ 14, 11.

<sup>14</sup> *See id.* ¶ 15. The GSMA IMEI database identifies stolen phones by their unique International Mobile Equipment Identity. But not all wireless carriers in the U.S. or abroad participate in these databases (just over 120 of 800 wireless carriers worldwide participate), and even those that do are not always as diligent as they could be. *See id.*

<sup>15</sup> *See id.* ¶ 13.

<sup>16</sup> Jessica Dolcourt, *Why Your iPhone and Android Phone Will Get More Expensive*, CNET (Nov. 11, 2018) <https://www.cnet.com/news/why-your-iphone-and-android-phone-will-get-more-expensive>; Schwed Decl. ¶ 8. The average cost of a stolen Verizon handset was \$697 in the beginning of 2017, and had grown to \$1038 by the end of 2018. *See* Schwed Decl. ¶ 8.

the 3G CDMA handsets used by Verizon and some other carriers did not work on the GSM networks found in most other countries.<sup>17</sup> Third, while generous device payment plans that require little or no down payment make it easier for legitimate customers to obtain new handsets, they also lower the barrier for criminals to obtain access to the same handsets.<sup>18</sup> Fourth, identity theft in general has been increasing due to the availability of high quality customer information that can now be obtained directly on the Internet, the “Dark Web,” or through “data brokers.”<sup>19</sup>

Verizon is also particularly susceptible to fraud because its devices carry a higher value on the black market. The value of a stolen handset on the black market depends, in part, on whether the handset can easily be resold, which in turn depends on whether the device is locked or unlocked.<sup>20</sup> An unlocked 4G LTE device has much greater value because it can be used on any carrier’s compatible 4G LTE network, including in foreign countries where a significant portion of illicit trade in stolen handsets occurs.<sup>21</sup> According to third-party trade-in services that Verizon tracks, the resale price of a Verizon device is consistently higher — in some cases by as much as \$100 — than the prices of devices of other carriers that lock their phones at the time of purchase, indicating that there is significantly greater value in an unlocked phone on the black market.<sup>22</sup>

---

<sup>17</sup> See Schwed Decl. ¶ 9.

<sup>18</sup> See *id.* ¶ 10.

<sup>19</sup> See *id.* ¶ 11.

<sup>20</sup> See Patrick Holland, *Unlocked Phones vs. Locked Ones: Everything You Need To Know*, CNET.com (July 9, 2018), <https://www.cnet.com/how-to/unlocked-phones-vs-locked-ones-everything-you-need-to-know> (“Since it’s unlocked, it usually has a higher resale value.”).

<sup>21</sup> See Matthew Shaer, *The Secret World of Stolen Smartphones, Where Business Is Booming*, Wired.com (Dec. 18, 2014), <https://www.wired.com/2014/12/where-stolen-smart-phones-go/>.

<sup>22</sup> See Schwed Decl. ¶ 12.

Handset theft harms both consumers and Verizon. The Commission has acknowledged, for example, that “[m]illions of dollars are lost each year due to subscriber fraud,” and that “[r]esolving subscriber fraud could develop into a long and difficult process for victims. It may take time to discover that subscriber fraud has occurred and even more time to prove that you did not incur the debts.”<sup>23</sup> Verizon’s data indicate that the number of consumers adversely affected by identity theft has increased from an average of 4800 customers per month in 2017 to approximately 7000 per month in 2018, an increase of 46 percent.<sup>24</sup> Consumers also are inconvenienced by the fraud controls that carriers have been forced to put in place, which are time-consuming and degrade the customer experience.<sup>25</sup> With respect to Verizon, the losses are also steep. As explained in the attached Schwed Declaration, handset fraud cost approximately \$190 million in 2018, up from approximately \$115 million in 2017. Verizon has lost almost 210,000 devices in 2018, up from a loss of approximately 155,000 devices in 2017.<sup>26</sup> These trends continue, as handset fraud cost Verizon \$34 million in January 2019, a 93 percent increase over January 2018.<sup>27</sup>

To combat handset fraud and theft, other large U.S. wireless carriers unlock 4G LTE devices only once they have been paid off in full, and only then on request and/or when certain criteria are satisfied.<sup>28</sup> AT&T will unlock a device 14 days after a request if the device is fully

---

<sup>23</sup> See source cited *supra* note 6.

<sup>24</sup> See Schwed Decl. ¶ 6.

<sup>25</sup> See *id.* ¶ 7.

<sup>26</sup> See *id.* ¶ 6.

<sup>27</sup> See *id.*

<sup>28</sup> See *id.* ¶ 4. See also sources cited *infra* notes 29-30 (outlining device locking policies of major U.S. wireless carriers).

paid off and has been in active service for at least 60 days.<sup>29</sup> T-Mobile and Sprint unlock devices automatically once they have been paid in full,<sup>30</sup> but both companies require a mandatory waiting period after activation before a phone can be unlocked — 50 days in the case of Sprint, and 40 days in the case of T-Mobile.<sup>31</sup>

Verizon seeks to implement a limited 60-day lock on new 4G LTE handsets that is less restrictive than both the handset unlocking provision of the CTIA Consumer Code for Wireless Service<sup>32</sup> and the locking policies of the other large wireless carriers. Verizon would unlock all such handsets automatically at the expiration of this 60-day period, except for those found to have been obtained illegally during that window. As set forth in the Schwed Declaration, 60 days provides Verizon sufficient time to determine that a new handset is associated with a legitimate customer. It allows both for the receipt of the first payment on an account and time for processing that payment to ensure that it was not reversed or otherwise cancelled after it was sent.<sup>33</sup> Unlike every other large U.S. wireless carrier, Verizon will unlock the device for legitimate customers after the 60-day period regardless of whether the device has been paid off

---

<sup>29</sup> AT&T, *Device Unlock Info*, <https://www.att.com/esupport/article.html#!/wireless/KM1262649>.

<sup>30</sup> T-Mobile, *Unlock Your Mobile Wireless Device*, <https://support.t-mobile.com/docs/DOC-1588>; Sprint, *Unlocking Your Sprint Device*, <https://www.sprint.com/en/legal/unlocking-your-sprint-device>.

<sup>31</sup> *See* sources cited *supra* note 30.

<sup>32</sup> *See* CTIA, *Consumer Code for Wireless Service*, Section 12: Mobile Wireless Device Unlocking, <https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service> (containing commitment by carriers to unlock mobile devices after fulfillment of the applicable postpaid service contract, device financing plan, or payment of applicable early termination fee).

<sup>33</sup> *See* Schwed Decl. ¶ 17.

by that time. Thus, even with this relief, Verizon will continue to lead the wireless industry in platform and device openness.

### **III. THE COMMISSION SHOULD DECLARE THAT VERIZON MAY LOCK PHONES TEMPORARILY TO REDUCE FRAUD AND IDENTITY THEFT**

Verizon has not implemented its proposed temporary lock on 4G LTE handsets because of ambiguity in the Commission’s rules governing C Block licensees like Verizon. Rule 27.16(e) provides that no C Block licensee “may disable features on handsets it provides to *customers*, to the extent such features are compliant with the licensee’s standards pursuant to paragraph (b) of this section, nor *configure* handsets it provides to prohibit use of such handsets on other providers’ networks.”<sup>34</sup> Because Verizon’s proposal would lock handsets only until such time as it can determine whether a handset belongs to a legitimate customer, however, it is unclear whether the handset locking rule even applies. Even if it does, a temporary lock does not “configure handsets . . . to prohibit use” on other providers’ networks. Legitimate customers will be able to use their handsets on other networks as soon as the 60 days expire.

The Commission may “issue a declaratory ruling terminating a controversy or removing uncertainty.”<sup>35</sup> As set forth below, Verizon requests that the Commission declare that a temporary 60-day lock on handsets is consistent with Rule 27.16(e).

#### **A. The Commission Should Declare That Temporary Locking of Handsets To Reduce Fraud and Identity Theft Does Not Violate Rule 27.16(e)**

Rule 27.16(e) prohibits Verizon from locking handsets of “customers.” The Commission should clarify that when an individual obtains a new account and new handset she does not automatically become a “customer” for purpose of the handset locking rule. Rather, a

---

<sup>34</sup> 47 C.F.R. § 27.16(e) (emphases added).

<sup>35</sup> 47 C.F.R. § 1.2.

“customer” relationship forms when an individual opens an account and obtains a new handset in good faith, with the intention to pay for the services on the account as well as the handset. The Commission should further declare that for purposes of determining whether an individual is a legitimate “customer” subject to the handset locking rule, it is reasonable for a carrier to impose a 60-day waiting period during which locking of a new 4G LTE handset is permitted, because such practices would not meaningfully affect legitimate “customers.”

A declaratory ruling is appropriate here because the Commission’s rules do not define “customer” for purposes of the handset locking rule, nor has the Commission expressly addressed the issue in this context. It is reasonable to declare that a “customer” is an individual who opens an account and obtains a new handset in good faith, with the intention to pay. In the context of tariffs, for example, a “customer” is typically defined as the individual or entity “responsible for payment.”<sup>36</sup> That is consistent with the standard dictionary definition of this term as well. For example, Black’s Law Dictionary defines a customer as “[o]ne who *regularly* or *repeatedly* makes purchases of, or has business dealings with, a tradesman or business. Ordinarily, one who has had *repeated* business dealings with another. A buyer, purchaser, consumer or patron.”<sup>37</sup>

---

<sup>36</sup> See, e.g., *AT&T Corp., Complainant, v. YMax Communications Corp., Defendant*, Memorandum Opinion and Order, 26 FCC Rcd 5742, ¶ 15 n.57 (2011); *American Satellite Corp. v. MCI Telecommunications Corp.*, Memorandum Opinion and Order, 57 FCC2d 1165, ¶ 5 (1976) (“Section B:1 of the tariff provides that a customer is a ‘. . . person, firm, corporation or other entity which orders services and responsible for payment of charges and compliance with [] tariff regulations.’”); *United Artists Payphone Corporation, Complainant, v. New York Telephone Company, and American Telephone and Telegraph Company, Defendants*, Memorandum Opinion and Order, 8 FCC Rcd 5563, ¶ 9 (1993) (“The term ‘customer’ is defined by the tariff as ‘the person or legal entity which orders [the service] (either directly or through an agent) and is responsible for payment of tariffed charges for services furnished to that Customer.’”).

<sup>37</sup> Black’s Law Dictionary 386 (6th ed. 1990) (emphases added).

It is particularly appropriate for the Commission to limit the definition of “customer” to someone “responsible for payment” in the context of wireless services and handsets. Today, most consumers obtain new 4G LTE handsets subject to two-year device payment plans that permit them to pay for the device on an amortized monthly basis over the life of that plan.<sup>38</sup> These plans — which have been introduced to meet consumer demands and in response to competitive forces — typically allow the subscriber to obtain a new handset with little or no money down, even though the cost of handsets has been rising.<sup>39</sup> Thus, even where an individual makes a small down payment to obtain a new handset, it is far from clear that the individual will be responsible for payment of the bulk cost of the device. In this context, it is entirely appropriate to distinguish between legitimate “customers” that obtain a new handset with the intent to pay for it, and those who obtain the handset with the intent to commit fraud and resell it on the black market.

For similar reasons, the Commission should also declare that for purposes of determining whether a new “customer” relationship has formed, Verizon may take reasonable steps — such as imposing a 60-day waiting period during which a new 4G LTE handset may be locked — to combat identity theft, first-party fraud, and related forms of handset theft. At the time Verizon provides a new 4G LTE handset to an individual, Verizon cannot be sure that the individual is who she claims and that she is obtaining the service and handset in good faith with the intention to pay. Thus, at the time of the actual transaction and despite the anti-fraud measures discussed above, Verizon is limited in its ability to ensure that an individual is a legitimate “customer” as opposed to someone using a stolen identity or otherwise engaged in fraud.

---

<sup>38</sup> See Schwed Decl. ¶ 10.

<sup>39</sup> See *id.* ¶¶ 8, 10.

Of course, as described above and in the Schwed Declaration, Verizon can and does take extensive precautions to try to sign up only legitimate customers, and is successful the overwhelming majority of the time.<sup>40</sup> But Verizon cannot definitively identify the small minority of fraudsters that manage to defy Verizon’s security mechanisms until the time that it receives the first payment on the account and is able to process that payment successfully.<sup>41</sup> It is only at that point that Verizon can be reasonably sure that the individual who obtained a new handset intends to pay for it, and is therefore a legitimate customer.<sup>42</sup>

**B. The Commission Should Declare That Temporary Locking of Handsets Does Not Constitute “Configuring” Handsets To Prohibit Use on Other Networks**

Similarly, or in the alternative, the Commission should declare that temporarily locking 4G LTE handsets as Verizon proposes does not amount to “configur[ing] handsets it provides to prohibit use of such handsets on other providers’ networks,” as set forth in Rule 27.16(e). “Configure” means “to set up for operation in a particular way,” or “to construct or arrange in a certain way.”<sup>43</sup> The 4G LTE handsets Verizon sells are not “set up” or “constructed” to operate only on Verizon’s network or to “prohibit” their legitimate use on other networks. Instead, Verizon proposes to lock those handsets temporarily, after which consumers could use those handsets on the networks of their choice, just as the C Block rules envision. Legitimate customers are unlikely even to notice the lock, and from their perspective the devices they purchase will effectively work on any compatible network.

---

<sup>40</sup> See Schwed Decl. ¶¶ 13-16.

<sup>41</sup> See *id.* ¶ 17.

<sup>42</sup> See *id.*

<sup>43</sup> Merriam-Webster.com, *Configure*, <https://www.merriam-webster.com/dictionary/configure>; *Webster’s New World College Dictionary*, 4th Ed. (Wiley Publishing, Inc. 2010). See also *The American Heritage Dictionary*, 5th Ed. (Houghton Mifflin Co. 2011) (“Configure” means “to design, arrange, set up, or shape with a view to specific application or uses.”).



**C. These Requested Declaratory Rulings Are Consistent with the Commission's Open Device Rules**

Issuing the declaratory rulings described above would not undermine the Commission's policies encouraging open platforms and open devices, but instead would advance them. As described further below, at the time the Commission adopted the C Block rules, including the handset locking rule, in 2007, its stated goals were to increase competition and choices for consumers of wireless services. Allowing Verizon to lock phones temporarily as proposed will further these goals. Verizon will continue to offer greater openness than other large wireless carriers by automatically unlocking its 4G LTE handsets after 60 days, regardless of whether they have been paid off in full, provided that it has determined the customer is legitimate. Under Verizon's proposal, consumers will still be able to use their 4G LTE handsets on other providers' networks as soon as the temporary locking period to help identify legitimate customers elapses. Thus, Verizon's proposed temporary locking is pro-consumer and pro-competitive and does not implicate the concerns about permanent locking of devices that the C Block rules and order addressed.

This approach also would have minimal, if any, effect on legitimate customers. Virtually all individuals who obtain new 4G LTE handsets from Verizon do so pursuant to a two-year device payment plan and stay with Verizon for that full two-year period in order to pay off their wireless device. Only a tiny fraction of legitimate customers seeks to end their new relationship with Verizon in the first 60 days after signing up for service, and those that do usually do so within the 14-day return period and return their phones to Verizon.<sup>44</sup> Thus, any legitimate

---

<sup>44</sup> See Schwed Decl. ¶ 18; Verizon Wireless, *Verizon Wireless Return Policy*, <https://www.verizonwireless.com/support/return-policy/>.

customers who seek to leave Verizon shortly after signing up would be able to do so, just as they may today.

#### **IV. IN THE ALTERNATIVE, THE COMMISSION SHOULD GRANT A PARTIAL WAIVER OF RULE 27.16(e) TO ALLOW VERIZON TO IMPLEMENT ITS TEMPORARY LOCKING PROPOSAL**

Should the Commission decide not to issue a declaratory ruling or decide that Verizon's proposal is inconsistent with Rule 27.16(e), the Commission should grant Verizon a partial waiver of the rule to implement its temporary locking proposal. The handset locking rule is not statutory. The Commission may therefore waive the rule "for good cause shown, in whole or in part, at any time."<sup>45</sup> The D.C. Circuit has held that a waiver is appropriate "where particular facts would make strict compliance inconsistent with the public interest."<sup>46</sup> In determining whether a waiver is in the public interest, the Commission may take into account considerations of hardship, equity, or more effective implementation of overall policy.<sup>47</sup> Applying these standards, there is abundant good cause for the Commission to grant Verizon a partial waiver of Rule 27.16(e) to implement a temporary lock to combat fraud and help determine legitimate customers.

A partial waiver is strongly in the public interest because it will help reduce handset fraud that is harming Verizon's customers, consumers generally, and Verizon itself. As described above and in the Schwed Declaration, identity theft and first-party fraud are costing Verizon and its customers approximately \$190 million per year, not even counting more difficult to quantify

---

<sup>45</sup> 47 C.F.R. § 1.3.

<sup>46</sup> *Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990); see *AT&T Corp. v. FCC*, 448 F.3d 426, 433 (D.C. Cir. 2006).

<sup>47</sup> See *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969).

harms such as greater inconvenience to consumers and greater risk of identity theft.<sup>48</sup> And these harms are occurring despite Verizon's extensive and ongoing efforts to combat this fraud.<sup>49</sup> A targeted partial waiver is necessary to further reduce these harms, which is precisely why other large wireless carriers have implemented even more stringent locking practices than those Verizon proposes.

Because Verizon is currently the only large U.S. wireless carrier to provide 4G LTE handsets unlocked immediately after sale, Verizon's customers suffer disproportionately from subscriber fraud and other related forms of theft. Verizon's customers face a greater risk of identity theft and other related forms of fraud. In fact, according to third-party trade-in services that Verizon tracks, the resale price of a Verizon device is typically higher than those of other carriers — in some cases by as much as \$100 — than the prices of comparable devices from carriers that lock their phones. This suggests there is significantly greater value in an unlocked phone on the black market, which increases the incentives for bad actors to target these devices and the risk of fraud to obtain unlocked devices.<sup>50</sup> A waiver would help eliminate the penalty that Verizon's customers face as a result of Verizon's implementation of the handset locking rule.

Finally, granting Verizon a partial waiver of the Commission's handset locking rule would not undermine, but instead would further, the policy rationales that motivated the Commission to adopt this rule. After 60 days, Verizon would unlock a new 4G LTE handset, thereby allowing the subscriber to switch carriers and activate that handset on a competitor's

---

<sup>48</sup> See Schwed Decl. ¶¶ 6-7.

<sup>49</sup> See *id.* ¶¶ 6, 13-16.

<sup>50</sup> See *id.* ¶ 12.

compatible network. The authentication and vetting process that Verizon would perform in this instance would help ensure that even subscribers who decide to switch providers are legitimate, thereby promoting fairer competition across the entire wireless ecosystem.

The Commission adopted the handset locking rule in 2007, as part of a broader package of “open platform” regulations governing the C block.<sup>51</sup> At that time, broadband wireless services were still fairly nascent — the Commission noted that U.S. wireless providers had just begun “moving beyond” 2G wireless technologies to 3G technologies,<sup>52</sup> and that “[a]s part of this evolution, ‘cell phones’ are evolving into multi-media devices capable of surfing the web, sending e-mails, playing songs, taking pictures, playing games, and streaming video.”<sup>53</sup> Indeed, the order was issued just a few months after the introduction of the first iPhone (which operated on 2G networks), and thus before a new age of smartphones revolutionized the industry.<sup>54</sup> The Commission noted it had “become increasingly concerned that certain practices in the wireless industry may constrain consumer access to wireless broadband networks and limit the services and functionalities provided to consumers by these networks.”<sup>55</sup>

None of the specific concerns the Commission expressed in adopting its open platform regulations relates to the handset locking rule, however, and nowhere did the Commission provide a specific basis for this rule. The Commission instead noted concerns that wireless

---

<sup>51</sup> *See Second C Block Order.*

<sup>52</sup> *Second C Block Order* ¶ 197.

<sup>53</sup> *Id.*

<sup>54</sup> *See, e.g., Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993*, Thirteenth Report, 24 FCC Rcd 6185, ¶ 164 (2009) (noting “AT&T’s June 2007 launch of Apple’s iPhone” and that “providers have responded to [this] development[] by introducing rival offerings”).

<sup>55</sup> *Second C Block Order* ¶ 198.

providers “appear to have required that equipment manufacturers disable certain capabilities in mobile devices, such as Wi-Fi capabilities,” without appropriate justification.<sup>56</sup> But nowhere did the Commission address the ability of consumers to switch wireless providers and whether locking was impeding that practice — to the contrary, the Commission noted that it had found that the wireless services market “is effectively competitive, and that competitive pressures continue to result in the introduction of innovative pricing plans and service offerings.”<sup>57</sup> The only mention of handset “locking” is in a single footnote that defines it as “one practice that *arguably* prevents consumers from migrating other technically compatible equipment from one wireless service provider to another,” and further noting that “[p]roviders claim that it is a practice designed to combat fraud.”<sup>58</sup>

In the intervening decade, wireless competition has continued to thrive, and the industry has rapidly implemented 4G technologies and is now working rapidly towards 5G.<sup>59</sup> This is occurring despite the fact that each of the other large U.S. wireless carriers besides Verizon locks their 4G LTE handsets at the time of purchase. The partial waiver of the handset locking rule that Verizon seeks would enable it to combat the epidemic of fraud and identity theft in ways less restrictive than those imposed by other wireless carriers, while protecting consumers and preserving their choices — a result squarely in the public interest.

---

<sup>56</sup> *Id.*

<sup>57</sup> *Id.* ¶ 200.

<sup>58</sup> *Id.* ¶ 190 n.430.

<sup>59</sup> *See, e.g., Communications Marketplace Report*, Report, GN Docket No. 18-231, WT Docket No. 18-203, MB Docket No. 17-214, MB Docket No. 18-227, IB Docket No. 18-251, FCC 18-181 (rel. Dec. 26, 2018), ¶¶ 19-20 & Fig. A-13 (noting the decline in the price of mobile wireless services, according to the Consumer Price Index, the decline of average revenue per unit, and an increase in the number of reported subscribers), ¶ 5 (“The mobile wireless industry is currently in the process of preparing for the introduction of 5G services . . .”).

## V. CONCLUSION

For all the foregoing reasons, the Commission should take one or more of the following steps:

- 1) The Commission should issue a declaratory ruling that a temporary 60-day lock on handsets is consistent with Rule 27.16(e);
- 2) To the extent the Commission decides not to issue a declaratory ruling or decides that Verizon's proposal is inconsistent with the handset locking rule in Rule 27.16(e), the Commission should grant Verizon a partial waiver of the rule to implement its temporary locking proposal.

Respectfully submitted,

Handwritten signature of Evan T. Leo in black ink, with the name written in a cursive style. The signature is positioned above a horizontal line.

Evan T. Leo

William H. Johnson  
*Of Counsel*

Tamara L Preiss  
VERIZON  
1300 I Street, N.W.  
Suite 500 East  
Washington, D.C. 20005  
(202) 515-2540

Evan Leo  
Sami M. Ahmed\*  
KELLOGG, HANSEN, TODD, FIGEL  
& FREDERICK, P.L.L.C.  
1615 M Street, N.W.  
Suite 400  
Washington, D.C. 20036  
(202) 326-7930

*\*Not admitted in the District of  
Columbia. Practice supervised by  
members of the firm.*

*Counsel for Verizon*

February 22, 2019

# **ATTACHMENT A**

## **DECLARATION OF STEPHEN SCHWED**



**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of

Verizon Request for Declaratory Ruling, or,  
in the Alternative, for Partial Waiver,  
Regarding the Handset Locking Rule for  
C Block Licensees

WT Docket No. 06-150

**DECLARATION OF STEPHEN SCHWED**

1. I, Stephen Schwed, am Manager of Long Term Fraud Strategy for Verizon (which as used here includes Cellco Partnership d/b/a Verizon Wireless). In this role, my responsibilities include overseeing policies regarding the contribution of data to the inter-carrier IMEI (International Mobile Equipment Identity) list of lost and stolen phones, and developing best practices for blacklisting devices lost to fraud or theft within the IMEI database. I am also actively engaged in the GSMA (Global Standard for Mobile Association) Device Security and Fraud Forum, the Security Groups and Communication Fraud Control Association (CFCA), and the CFCA Consumer Education Committee, which I chair. I began my telecommunications career in 1997 with Bell Atlantic Mobile, a predecessor company to Verizon, as a Collections Specialist. From 2000 to 2004, I was a member of Verizon's Executive Relations group for the Philadelphia Region. After a brief stint as the Northeast Area Indirect Point of Sale Consultant in 2005, I returned to manage the Executive Relations Team. In 2013, I began work as a Process Manager in Telecommunications Fraud to address policy and process issues related to fraud and other losses. I officially joined Verizon's Fraud Strategy Team in 2015.

2. I have been asked to discuss the issues that Verizon and its customers face with fraud and theft, including identity theft, involving 4G LTE handsets. First, I describe Verizon's

policies with respect to unlocking 4G LTE handsets and contrast them to the practices of other large U.S. wireless providers. Second, I discuss the fraud and theft of 4G LTE handsets that Verizon has experienced despite the extensive measures it has taken to prevent such crime. Third, I explain how being allowed to lock phones for a temporary initial period would help Verizon identify legitimate customers and reduce fraud and theft associated with 4G LTE handsets.

3. Each 4G LTE handset may be provided to a purchaser “locked,” so that it works with only one Subscriber Identification Module (“SIM”) card that is tied to a specific carrier’s network, or “unlocked,” to operate with any SIM card on any carrier’s compatible 4G network. Verizon is currently the only large U.S. wireless carrier that provides 4G LTE handsets to subscribers unlocked at the time of purchase, thereby enabling these devices to be used immediately on another carrier’s 4G LTE network. Although Verizon receives 4G LTE handsets locked from the manufacturer, Verizon unlocks them upon sale.

4. Neither Sprint, T-Mobile, nor AT&T provides 4G LTE handsets unlocked at the time of purchase to subscribers. These other carriers unlock 4G LTE handsets only once they have been paid in full, and only then on request and/or when certain criteria are satisfied. AT&T will unlock a device 14 days after a request if the device is fully paid off and has been in active service for at least 60 days.<sup>1</sup> T-Mobile and Sprint unlock devices automatically once they have been paid in full, but both companies require a mandatory waiting period after activation before a phone can be unlocked — 50 days in the case of Sprint, and 40 days in the case of T-Mobile.<sup>2</sup>

---

<sup>1</sup> AT&T, *Device Unlock Info*, <https://www.att.com/esupport/article.html#!/wireless/KM1262649>.

<sup>2</sup> T-Mobile, *Unlock Your Mobile Wireless Device*, <https://support.t-mobile.com/docs/DOC-1588>; Sprint, *Unlocking Your Sprint Device*, <https://www.sprint.com/en/legal/unlocking-your-sprint-device>.

5. Verizon and its subscribers are experiencing significant and growing theft of 4G LTE handsets and related fraud. There are three primary types of fraud used to steal 4G LTE devices: (i) identity theft, in which an individual signs up for service and obtains new handsets using a fraudulently obtained identity and credit information or by impersonating a legitimate customer to add devices on that customer's account; (ii) first-party fraud, in which an individual uses his or her own identity to acquire new handsets legally but with the intent of never paying for the devices; such individuals are often participants in aggregation schemes that orchestrate the fraud, giving the individual a portion of the stolen proceeds and coaching them on how to disclaim the debt; and (iii) synthetic identity, in which a profile of information is created using credit report practices that allow sharing of credit-history data of a legitimate individual paired with a fictitious name and identity. For its internal data and for the purposes of this declaration, Verizon groups synthetic identity theft within the broader category of identity theft.

6. Verizon has tracked the losses of 4G handsets it has experienced over time, and these data show that such theft is a significant and growing problem harming Verizon and its customers. Handset fraud was minimal in 2015, began to ramp up in 2016, and has grown significantly both in 2017 and 2018. Our data indicate that Verizon lost approximately 210,000 devices in 2018, up from a loss of approximately 155,000 devices in 2017. Verizon estimates that handset fraud cost nearly \$190 million in 2018, up from approximately \$115 million in 2017. Verizon's data further indicate that the number of consumers adversely affected by identity theft has increased from an average of 4800 per month in 2017 to approximately 7000 per month in 2018, an increase of 46% year over year. These trends continue, as handset fraud cost Verizon \$34 million in January 2019, a 93% increase over January 2018.

7. Identity theft and other forms of handset fraud not only directly affect many subscribers, but they also indirectly harm consumers more generally. Losses due to fraud affect carriers' credit policies and the type and extent of credit that can be offered, which can make it more difficult for some consumers to obtain access to wireless service and the latest handsets. In addition, although carriers are ultimately responsible for cleaning up the credit of consumers who are affected by handset fraud, that process could inconvenience consumers. Rising fraud also requires carriers to implement more stringent safeguards and fraud controls, which degrade the customer experience in numerous ways. For example, such mechanisms may increase the time and complexity of validating an identity digitally or over the phone. Strict anti-fraud measures may also delay or prevent legitimate customers from obtaining a device in some cases.

8. Handset theft is increasing for several reasons. First, the cost of such devices has skyrocketed. Since 2015 alone, the average retail price of a new handset has increased by approximately 50%, with the most popular devices now retailing for \$1000 or more. The average cost of a stolen Verizon handset was \$697 in the beginning of 2017, and had grown to \$1038 by the end of 2018.

9. Second, 4G LTE devices sold in the U.S. are compatible with 4G LTE networks abroad, which has created a worldwide market for resold 4G LTE handsets. Once a 4G LTE handset is unlocked, it can immediately be used on any carrier's compatible 4G LTE network, anywhere in the world, due to the interoperability among 4G LTE networks. This contrasts with 3G technology, for which there were competing standards (*e.g.*, EDGE, UMTS, CDMA) and interoperability issues among some of them. The 3G CDMA handsets used by Verizon and some other carriers thus did not work on the GSM networks found in most other countries.

10. Third, it has become easier for criminals to obtain access to handsets due to the change from offering subsidized devices to providing generous device payment plans that require little or no down payment. Today, most consumers obtain new 4G LTE handsets subject to two-year device payment plans that permit them to pay for the device on an interest-free, amortized monthly basis over the life of the plan. Enabling consumers to obtain valuable new handsets with a minimal down payment and an interest-free loan helps promote the expansion of broadband wireless services, but it also facilitates the theft of new handsets as thieves do not need to make a material investment before gaining control over a new handset that they may turn around and resell on the black market.

11. Fourth, high-quality consumer information is becoming ubiquitous, which makes consumers more susceptible to identity fraud. More information about consumers is readily available than many consumers realize. High quality consumer information can now be obtained directly on the Internet, on the “Dark Web,” or through “data brokers.” Social media and other resources may be used to assist thieves in determining responses to private Knowledge-Based Authentication (“KBA”) questions, such as the name of the individual’s first pet or mother’s maiden name. In addition to the information that is publicly available, private and confidential information may be inadvertently revealed through, for example, social engineering or large data breaches, and once this occurs, it is difficult to remedy. Several large-scale data breaches have recently occurred, involving Equifax, Marriott, and others, revealing sensitive consumer information that thieves are able to leverage.

12. Verizon and its customers are generally even more likely to be targets of fraud and device theft than other large wireless carriers and their customers. Verizon is the only large wireless carrier that provides phones unlocked at the time of purchase, which makes these

devices especially appealing to thieves.<sup>3</sup> This is borne out by the fact that, according to third-party trade-in services that Verizon tracks, the resale value of a Verizon device is typically higher than those of other carriers. The premium for Verizon devices is often as high as \$100, demonstrating the increased value of the unlocked devices that Verizon provides compared to the locked devices of other carriers. And because Verizon's handsets have greater value on the black market, bad actors have greater incentives to obtain these devices through fraud.

13. Verizon continues to develop and undertake extensive measures to combat fraud and theft of its devices, but these mechanisms have limitations. For example, while some of these tools have helped reduce identity theft, they are less effective at combatting first-party fraud, in which a purchaser uses his or her legitimate identity to obtain the phone but without any intention to pay for it. In addition, while Verizon and other carriers are continually investing in ways to develop new fraud detection tools, thieves are likewise working to develop new ways to thwart fraud detection mechanisms and steal handsets, which makes eliminating fraud even more difficult.

14. When a new or existing subscriber seeks a new handset, Verizon authenticates the purchaser by seeking identification and credit information. With the assistance of outside vendors, Verizon runs a credit check and a red-flags test to help ensure that the subscribers are who they claim to be and that they are likely to pay for the devices they have ordered. Additionally, Verizon employs a proprietary fraud decision engine that evaluates over 140 different attributes associated with digital, telesales, and face-to-face transactions. For each transaction, the engine calculates and assigns a fraud risk score by examining different attributes such as the IP address, shipping address mismatches, and credit card history. Based on the risk

---

<sup>3</sup> See *infra* ¶¶ 3, 4.

score, Verizon may take additional steps to authenticate the subscribers, such as requiring responses to KBA questions. Verizon is also investing in new technology to identify “fake” identification used in face-to-face transactions.

15. Verizon also participates in national and global databases to track and share information about stolen and fraudulently obtained devices, which are intended to deter and prevent handset theft. The GSMA IMEI database contains the serial numbers of stolen devices, which wireless carriers may (and should) consult before activating a device. Worldwide, however, only a minority of wireless carriers (approximately 120 out of 800) participate in this database, which means there are many countries where it is easy to activate a stolen device. In addition, among those carriers that do participate, some share information and enforce the blacklist only in connection with other local carriers rather than with all global participants of the database.

16. In addition to the steps described above, Verizon is investing in new ways to detect fraud and eliminate handset theft. For example, Verizon is investing in big data analyses and artificial intelligence more quickly to identify trends and changes in trends that may indicate fraud. But there is only so much that Verizon can control. For example, Verizon and other carriers have no ability to disable (or “brick”) a phone that has been reported stolen, which is a step that would help prevent theft by making it economically unattractive. This limitation is imposed by the device manufacturers.

17. Based on my experience, the ability to lock phones temporarily for 60 days after purchase would significantly help Verizon combat identity theft, first-party fraud, and other forms of handset theft that Verizon faces. This time would allow Verizon to determine that an individual obtaining a handset is a legitimate customer that intends to pay for it. Verizon can

only make such a determination once it both receives the first payment on the account and processes that payment successfully to ensure that it was not reversed or otherwise cancelled after it was sent. This process takes at least 60 days.

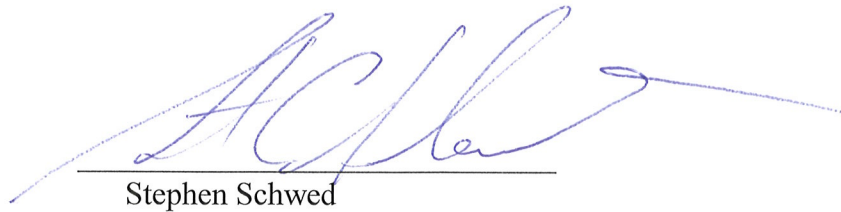
18. A temporary 60-day lock would not have a material impact on consumers or meaningfully restrict consumers from switching carriers. Only a tiny fraction of Verizon customers port their numbers or change carriers within the first 60 days of service, meaning a temporary lock would, at most, impact a very small number of customers seeking to switch carriers. Those customers that seek to end their new relationship with Verizon in the first 60 days after signing up for service usually do so within the 14-day return period and return their phones to Verizon. Following the 60-day period, moreover, Verizon subscribers would be free to switch carriers and to take their handset with them and activate it on a competitor's network. Verizon's ability to impose a 60-day lock on devices would help deter fraud and theft against Verizon's customers, reduce the company's losses, and enable it to offer services to a broader range of consumers.

\* \* \*



I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on February 21, 2019



A handwritten signature in blue ink, appearing to read 'S. Schwed', is written over a horizontal line. The signature is stylized and cursive.

Stephen Schwed