

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
Washington D.C.**

_____	)	
	)	
In the Matter of	)	
	)	
Implementation of the Telecommunications	)	
Act of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer	)	Docket No. 96-115
Proprietary Network Information and Other	)	
Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security	)	RM - 11277
and Authentication Standards for Access to	)	
Customer Proprietary Network Information	)	
	)	
_____	)	

**REPLY COMMENTS OF VIRGIN MOBILE USA, LLC**

Peter Lurie  
Virgin Mobile USA, LLC  
10 Independence Blvd  
Warren, NJ 07059

Antoinette C. Bush  
John M. Beahn  
Skadden, Arps, Slate, Meagher & Flom LLP  
1440 New York Avenue  
Washington D.C. 20005

*Counsel to Virgin Mobile USA, LLC*

Date: June 2, 2006

## SUMMARY

Virgin Mobile USA, LLC applauds the Commission for commencing this proceeding to respond to concerns related to the protection of Customer Proprietary Network Information ("CPNI") and other forms of customer-sensitive information. Safeguarding customer-sensitive information remains a top priority at Virgin Mobile and, as demonstrated herein, is a responsibility that Virgin Mobile takes seriously. Virgin Mobile understands the Commission's desire to prevent the ongoing unauthorized disclosure of customer-sensitive information, including CPNI. Accordingly, Virgin Mobile supports the proposals justified by the record compiled in this proceeding that would effectively diminish instances of unauthorized access to CPNI while also providing carriers with the ability to tailor each proposal's requirements to their specific business operations. As a result, Virgin Mobile supports an optional consumer-set password system and a flexible customer notification obligation where a carrier has confirmed that a customer's CPNI or other sensitive information has been compromised.

Virgin Mobile believes that the factual record compiled in this proceeding does not support the imposition of sweeping regulations governing carrier security procedures. Indeed, many of the proposals described in the Notice would not prevent the unauthorized disclosure of CPNI. Adoption of a "one-size-fits-all" solution to carrier security, moreover, remains unwarranted and would not better protect the security of customer information. More important, this approach could inhibit innovation in carrier security mechanisms by "locking-in" certain practices and technologies. Such a result would prevent carriers from responding to future threats to the security of customer-sensitive information and could inhibit carriers' ability to modify their risk assessment and security response mechanisms to address evolving threats or changes in technology.

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
Washington D.C.**

_____	)	
	)	
In the Matter of	)	
	)	
Implementation of the Telecommunications	)	
Act of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer	)	Docket No. 96-115
Proprietary Network Information and Other	)	
Customer Information	)	
	)	
Petition for Rulemaking to Enhance Security	)	RM - 11277
and Authentication Standards for Access to	)	
Customer Proprietary Network Information	)	
	)	
_____	)	

**REPLY COMMENTS OF VIRGIN MOBILE USA, LLC**

Virgin Mobile, USA, LLC ("Virgin Mobile"), by undersigned counsel, respectfully submits these Reply Comments in response to the Notice of Proposed Rulemaking ("Notice") released in the above-captioned proceeding on February 14, 2006.<sup>1</sup> Virgin Mobile commends the Federal Communications Commission ("FCC" or "Commission") for commencing this proceeding to examine the need for increased security measures to protect customer-sensitive information, including customer proprietary network information ("CPNI"). As detailed below, Virgin Mobile endorses those flexible proposals supported by the record that would reduce the

---

<sup>1</sup> See *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and other Customer Information and Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket 96-115, RM-11277, *Notice of Proposed Rulemaking* (rel. February 14, 2006).

unauthorized disclosure of customer-sensitive information. Virgin Mobile believes, however, that the factual circumstances established in this proceeding do not support implementation of the sweeping regulations proposed in the Notice. Indeed, many of the proposals described in the Notice would not prevent the ongoing unauthorized disclosure of customer-sensitive information, including CPNI.

## I. INTRODUCTION

### A. Company Background

Virgin Mobile is an innovative carrier that provides its customers with fun, lifestyle voice and data features and unique, prepaid service plans. Virgin Mobile's simple and straightforward pricing, along with its unique customer service model, has redefined the prepaid wireless marketplace and contributed greatly to its growth. The company currently offers three prepaid service plans. Each of these plans provides customers with easy methods by which they can replenish (or "Top-up") their accounts, including through their handset, online with a credit card, or with a Top-up card available at over 70,000 locations nationwide including BestBuy, WalMart, Radio Shack, and Target.

Virgin Mobile's highly-regarded customer service model further simplifies its customers' wireless experience. In contrast to most wireless providers, Virgin Mobile does not require its customers to enter into a long-term service contract to initiate service. The prepaid nature of Virgin Mobile's service offering also obviates the need for a credit check or the mandatory collection and review of personally-identifiable customer information (e.g., social security number) prior to the commencement of service. As a result, Virgin Mobile does not require certain customer-sensitive information that other carriers demand from their customers.

Contrary to most carriers' operations, Virgin Mobile also does not offer its customers paper bills or account statements. Instead, customer account information is available online or through Virgin Mobile's customer care hotline. The account information available to customers includes Top-up information, the time, date, and length of the customer's most recent calls, as well as their account balance information and any other services or features (e.g., ringtones) that the customer may have purchased. Virgin Mobile's customers prefer electronic or telephonic account information to the complex and confusing monthly paper bills and account statements provided by most wireless carriers.<sup>2</sup> As further described below, this simplified account management system reduces the potential for the unauthorized disclosure of customer-sensitive information, including the release of CPNI.

**B. Company Security Procedures.**

Virgin Mobile complies with all applicable federal and state statutes and regulations, including FCC requirements governing the protection, use, and disclosure of CPNI. Access to CPNI and personally-identifiable customer information is restricted only to those employees and agents necessary to provide or market Virgin Mobile's services and products. Virgin Mobile trains its employees and agents with access to CPNI on the proper use and handling of customer-sensitive information. All vendors that obtain any CPNI or personally-identifiable customer information also are contractually bound to keep all such information confidential, use such information only to provide services to the company, and immediately disclose any security breach regarding such information to Virgin Mobile. Virgin Mobile has disciplinary procedures in place should any Virgin Mobile employee or agent violate the company's policies with respect

---

<sup>2</sup> Because its customers prefer online account information, Virgin Mobile receives very few requests for paper copies of account information.

to the use and disclosure of customer CPNI. A limited number of employees have access to customer CPNI.

In addition to these legal obligations, Virgin Mobile has implemented supplemental security procedures and technical systems to further protect customer-sensitive information from unwarranted disclosure.

1. vKey

Virgin Mobile maintains a 100-percent password-protected account management system. Pursuant to this system, a customer must provide a proper Virgin Mobile phone number and associated password (a "vKey") to access any customer account information. During the service activation process, Virgin Mobile requires customers to select an alphanumeric, six-digit vKey that only the customer would know. (Virgin Mobile advises its customers not to share their vKey with any other individual for any reason.) Customers may change their vKey at any time either online or through the Virgin Mobile customer hotline. A customer must provide their telephone number and vKey irrespective of whether the customer attempts to access account information online or through Virgin Mobile's customer hotline. Virgin Mobile customer service representatives are trained to deny access to any individual who does not provide both the Virgin Mobile wireless number and the relevant vKey. Once a customer properly enters their telephone number and vKey, the customer can access any of his or her account information, including a list of their most-recent calls, Top-up information, account balance, and other personally-identifiable information.

In the event that a customer misplaces or forgets their vKey, Virgin Mobile requires the customer to answer a vKey reminder question. During the service activation process, Virgin Mobile provides customers with a pull-down menu of potential reminder questions; the answer

to which only the customer would know.<sup>3</sup> The customer must provide the answer to this question any time the customer forgets or misplaces their vKey. In the online context, should the customer fail to properly answer their secret question, the customer will be denied access to the account information. For telephone requests, Virgin Mobile customer care personnel are trained to deny access to the account in the event that a customer misplaces or forgets their vKey. In situations in which the customer does not have the vKey or the answer to their secret question, Virgin Mobile customer care personnel will provide the customer with a new vKey only if the customer provides other account information that only the customer would know. For instance the customer could provide the date and amount of their most recent Top-up.

## 2. Company Policies.

Virgin Mobile maintains a rigorous internal policy governing external requests for customer-sensitive information, as well as a privacy policy which manages the handling of customer-sensitive information. Virgin Mobile trains company personnel in accordance with these policies, and all employees must annually verify their familiarity with the procedures set forth therein. Violation of either policy is grounds for immediate termination.

The policy governing external requests for customer-sensitive information sets forth the procedures by which Virgin Mobile personnel must respond to requests for access to and the production of customer-sensitive information from i) current Virgin Mobile customers, ii) law enforcement agencies, and iii) third-party non-governmental individuals (e.g., relatives, third-party attorneys, etc.). The policy details the form of authorization required and a description of the procedures that company personnel must follow to ensure that any disclosure of customer-sensitive information is undertaken pursuant to the company's obligations under current law and

---

<sup>3</sup> Alternatively, the customer can create their own reminder question and answer.

its privacy policy. By establishing clear and coherent procedures for the disclosure of customer-sensitive information, this policy ensures the consistent protection of CPNI and other customer-sensitive information and documentation.

Virgin Mobile's privacy policy informs customers of the methods by which Virgin Mobile collects information from them, the potential uses of this information, and the customers' rights regarding any personally-identifiable information. Under this policy, Virgin Mobile may collect certain personally-identifiable information from the customer during the service activation process, including the customer's name, address, and credit card information. The privacy policy also restricts Virgin Mobile's use of this information to those instances necessary to provide or market services to the customer. Finally, the policy provides customers with the ability to remove their personally-identifiable information, choose whether to receive marketing information from Virgin Mobile or its business partners, and select the methods by which Virgin Mobile may contact the customer.

## II. POTENTIAL DISCLOSURE OF CUSTOMER INFORMATION

The Commission's Notice arises from an August 2005 Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC").<sup>4</sup> In its Petition, EPIC expressed concerns about the sufficiency of carrier practices regarding the protection of CPNI, especially with respect to the unauthorized disclosure of customer call records. EPIC's Petition identified numerous online data brokers that purport to sell the call records of wireline and wireless customers. EPIC alleges that these data brokers exploit inadequate carrier security mechanisms

---

<sup>4</sup> See *Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket No. 96-115 (filed Aug. 30, 2005)(hereinafter, "EPIC Petition").

to obtain unauthorized access to customer-sensitive information, including customer call records.<sup>5</sup>

As a result of EPIC's allegations, the Commission initiated the instant proceeding "to determine whether enhanced security and authentication standards for access to customer telephone records are warranted."<sup>6</sup> To this end, the Notice requests information on the extent of the unauthorized disclosure of customer-sensitive information, with a specific focus on the methods by which third parties gain unauthorized access to customer-sensitive information. Other commenters in this proceeding have confirmed the existence of the practices described in EPIC's Petition, indicating that unauthorized individuals attempt to gain access to customer accounts.<sup>7</sup> These commenters maintain that the practice of so-called "pretexting," by which online data brokers trick consumer service representatives into disclosing customer-sensitive information, appears to be the primary source of unauthorized access.<sup>8</sup>

Virgin Mobile has alerted its customer service representatives to determine whether Virgin Mobile has experienced any similar activities. While Virgin Mobile does not doubt the existence of these activities, to its knowledge, Virgin Mobile has not experienced any pretexting activities. Virgin Mobile also has not discovered other attempts by unauthorized third parties to gain access to customer-sensitive information. In this regard, Virgin Mobile has not detected any intrusions of its information technology ("IT") systems or "hacks" of its IT security mechanisms.

---

<sup>5</sup> See *EPIC Petition* at p. 1.

<sup>6</sup> *Notice* at ¶ 1.

<sup>7</sup> See *Cingular Comments* at p.10-12.

<sup>8</sup> See *Cingular Comments* at p.13; *Sprint Nextel Comments* at p.4.

### III. ANALYSIS OF PROPOSALS

#### A. Scale of Data Broker Activities Does not Justify Imposition of Sweeping Regulations.

Virgin Mobile applauds the Commission's prompt response to the practices and activities described in the EPIC Petition and in various filings submitted in this proceeding. Virgin Mobile also understands the Commission's desire to prevent the unauthorized disclosure of customer-sensitive information, including CPNI. Virgin Mobile believes, however, that the imposition of sweeping regulations governing carrier security procedures is not supported by the record in this proceeding. The filings submitted in this proceeding confirm that the unauthorized disclosure of CPNI is primarily confined to pretexting calls made by online data brokers. With that in mind, many of the proposals described in the Notice would fail to prevent the primary source of the unauthorized disclosure of customer call records.<sup>9</sup> Accordingly, the Commission should narrow the focus of this proceeding to target the specific concerns raised by data broker activities and supported by the factual record contained herein. To this end, Virgin Mobile supports an optional consumer-set password system and a flexible customer notification obligation where a carrier has confirmed that a customer's CPNI or other sensitive information has been compromised.

Virgin Mobile believes that a "one-size-fits-all" approach to carrier security would be unwise and would eliminate the regulatory flexibility that is vital in responding to potential security threats. Mandating specific solutions for the security of customer information, moreover, would inhibit innovation in carrier security mechanisms and dissuade carriers from experimenting with new security mechanisms. Such an outcome could prevent carriers from

---

<sup>9</sup> Virgin Mobile's use of passwords from all customers provides additional protection against this practice.

responding to future threats to the security of customer-sensitive information. Indeed, prescriptive regulation may inhibit carriers' ability to modify their risk assessment and security response mechanisms to address evolving threats or changes in technology. Requiring specific industry-wide solutions to protect customer information also could serve to "lock-in" certain practices and technologies, standardizing security procedures and reducing the effectiveness of individual carrier safeguards.

B. Changes to Opt-Out Mechanisms are Unwarranted.

The Commission questions whether the existing opt-out regime for use and disclosure of CPNI sufficiently protects the security of CPNI.<sup>10</sup> In this regard, the Notice requests comment on whether imposition of a mandatory opt-in regime for all use and disclosure of CPNI would better protect customers' privacy.

Virgin Mobile strongly believes that changes to the FCC's current opt-out regime are unwarranted. Imposition of prohibitive regulations requiring opt-in approval for all use and disclosure of CPNI would not prevent data broker access to CPNI. Indeed, no commenter in this proceeding (including Virgin Mobile) has identified a situation in which the current opt-out system has jeopardized the security of CPNI, or other customer-sensitive information. Absent such a factual record, the Commission can not impose such a sweeping change to its carrier security procedures. Virgin Mobile also agrees with other commenters that have noted that a mandatory opt-in approach would raise constitutional concerns in light of the Tenth Circuit's ruling in U.S. West v. FCC.<sup>11</sup>

---

<sup>10</sup> See *Notice* at ¶ 12.

<sup>11</sup> See *Verizon Comments* at p. 23.

Virgin Mobile believes that EPIC and the other privacy and consumer advocate groups are attempting to use this proceeding to revisit long-settled issues related to mandatory opt-in consent for all applications and disclosures of CPNI.<sup>12</sup> In its deliberations of these issues, the Commission should note that these parties have failed to address the fact that the existing opt-out regulations have been effective in preventing unauthorized access and disclosure of CPNI.

C. Comments on EPIC's Proposals.

In its Petition, EPIC alleges that data brokers exploit inadequate carrier security mechanisms to gain unauthorized access to CPNI and other customer-sensitive information.<sup>13</sup> The Notice requests comment on five specific security measures that EPIC proposes would enhance carrier security procedures: mandatory consumer-set passwords, adoption of audit trails, encryption requirements, limitations on data retention, and customer notification regulations.

1. Mandatory Consumer-Set Password System.

As described above, Virgin Mobile has been an innovator in carrier security procedures and was the first nationwide carrier to employ a mandatory consumer-set password system. Virgin Mobile believes that the user-friendly nature of the vKey has contributed greatly to the company's success in implementing the system. Virgin Mobile's streamlined carrier-customer relationship model in which customers can only obtain account information online or telephonically also has driven customer acceptance of the vKey. While Virgin Mobile has successfully implemented a mandatory consumer-set password system, Virgin Mobile cautions the Commission against mandating such a system for all service providers.

---

<sup>12</sup> See *Privacy Rights Clearinghouse Comments* at p.4.

<sup>13</sup> See *EPIC Petition* at p. 5.

Carriers should be free to adopt the security mechanisms that best fit their carrier-customer relationship model. In this regard, imposing a mandatory consumer-set password requirement may prevent the development of additional innovative customer authentication mechanisms. As many commenters have noted, a mandatory password system would impose significant implementation costs on carriers.<sup>14</sup> Carriers also would face substantial costs in educating customers on the parameters of such a system. Most important, adoption of a mandatory consumer-set password system could pose significant challenges to customers, especially customers unaccustomed to the use of a password verification system for use of wireless services.

Virgin Mobile supports the Commission's goal to provide customers with better control over their account information. To this end, Virgin Mobile supports a requirement that carriers provide customers with the option of implementing a password protection system for their account information. Such a requirement would provide those customers receptive to such a system with the additional protection that they desire, while not contravening other customer preferences against mandatory passwords.

## 2. Audit Trail.

EPIC also suggests that the Commission should require carriers to record all instances in which customer-sensitive information has been accessed and disclosed and to provide customers with this information.<sup>15</sup> From Virgin Mobile's perspective, a mandatory audit trail and customer notice requirement would be unduly burdensome to employ and costly to implement. In this regard, Virgin Mobile agrees with other carriers in this proceeding who have argued that the

---

<sup>14</sup> See *Verizon Comments* at 5-6; *Cingular Comments* at p.19-20; *AT&T Comments* at p.10.

<sup>15</sup> See *EPIC Petition* at 11.

Commission should permit carriers to tailor their recordkeeping procedures to their own business needs and financial constraints.<sup>16</sup> Requiring carriers to record all instances in which their CPNI was accessed and/or disclosed would impose needless administrative burdens on carriers without the corresponding benefit of preventing the unauthorized disclosure of CPNI. Indeed, a mandatory audit trail requirement lacks any connection to the factual issues raised in this proceeding and would not prevent unauthorized access to CPNI.

### 3. Encryption.

EPIC proposes that any customer-sensitive information stored by carriers should be encrypted.<sup>17</sup> As described above, Virgin Mobile already undertakes significant procedures, including encryption techniques, to guard against the unauthorized disclosure of customer-sensitive information, which Virgin Mobile believes inhibits intrusion of carrier IT systems. As other commenters have noted in this proceeding, however, "hacking" of IT systems has not been the primary source of unauthorized disclosure of customer-sensitive information.<sup>18</sup> A mandatory encryption requirement could lock-in current practices and technologies, thereby thwarting the development and deployment of new encryption technologies. A mandatory encryption requirement would standardize security procedures and reduce the effectiveness of individual carrier safeguards. In this manner, mandated encryption practices could restrain carriers' ability to respond as future threats to the security of customer-sensitive information evolve.

---

<sup>16</sup> See *Sprint Nextel Comments* at p.13.

<sup>17</sup> See *EPIC Petition* at 11.

<sup>18</sup> See *Cingular Comments* at p.23; *Verizon Comments* at p. 16; *AT&T Comments* at p.15.

#### 4. Limiting Data Retention.

Fourth, EPIC indicates that deletion of call records after a certain period of time would help to protect customer-sensitive information from unwarranted disclosure.<sup>19</sup> While Virgin Mobile does not oppose mandatory timeframes for the destruction of customer-sensitive information, Virgin Mobile does question the advantages of such a requirement. As an initial matter, Virgin Mobile retains customer call records for 18 months in accordance with FCC regulation for the retention of telephone toll records.<sup>20</sup> As other commenters have noted, a mandatory destruction requirement could reduce carriers' ability to respond to law enforcement requests and third-party subpoenas.<sup>21</sup> Mandatory retention limits also would not prevent the unauthorized disclosure of CPNI. The record in this proceeding confirms that data brokers covet recent CPNI, somewhat obviating the need to impose a mandatory destruction requirement for more dated CPNI.

#### 5. Notice.

Finally, EPIC proposes to require carriers to notify customers when the security of their CPNI may have been breached. Virgin Mobile supports a customer notification requirement, but only in situations in which a carrier has confirmed that a customer's CPNI or other sensitive information has been compromised.<sup>22</sup> Requiring customer notification for all situations in which customer-sensitive information "may" have been breached as proposed by EPIC would desensitize customers to more legitimate notifications. In addition, any customer notification

---

<sup>19</sup> See *EPIC Petition* at 11.

<sup>20</sup> See 47 C.F.R. § 42.6.

<sup>21</sup> See generally, *Department of Homeland Security, Department of Justice Comments*.

<sup>22</sup> In Virgin Mobile's view, unauthorized disclosure of publicly-available information, such as customer name and billing address, would not justify customer notification.

requirement that the Commission adopts should provide carriers with sufficient flexibility as to the timing and form of any customer notification. For instance, the Commission should not mandate bill inserts or written notification and should permit electronic customer notification. As noted above, Virgin Mobile does not provide paper bills or account statements to customers. Any regulatory requirement requiring written notification to customers would impose significant costs on Virgin Mobile and its customers.

#### V. CONCLUSION

Virgin Mobile applauds the Commission for commencing this proceeding to respond to concerns related to the protection of CPNI and other forms of customer-sensitive information. However, imposition of sweeping regulations governing carrier security procedures is not supported by the record in this proceeding. Adoption of a "one-size-fits-all" solution to carrier security, moreover, remains unwarranted and would not better protect the security of customer information.

Respectfully submitted,

By: /s/\_\_\_\_\_  
Antoinette C. Bush  
John M. Beahn  
Skadden, Arps, Slate, Meagher & Flom LLP  
1440 New York Avenue  
Washington D.C. 20005

*Counsel to Virgin Mobile USA, LLC*

Peter Lurie  
Virgin Mobile USA, LLC  
10 Independence Blvd  
Warren, NJ 07059