



EX PARTE OR LATE FILED

ORIGINAL

October 31, 2006

FILED/ACCEPTED

OCT 31 2006

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Federal Communications Commission
Office of the Secretary

**Re: Notice of Ex Parte Presentation, CC Docket No. 96-115
Telecommunications Carriers' Use of Customer Proprietary Network Information
and Other Customer Information**

Dear Ms. Dortch:

Unscrupulous individuals and companies have been engaging in a process called "pretexting" to obtain customer call detail records. They defraud carriers to obtain information about the call records of consumers for their own personal profit. This activity threatens carriers' customers' privacy, and may serve as a foundation for further illegal or unscrupulous activity.

The following companies have joined together voluntarily to share best practices and develop strategies for preventing this fraud and protecting privacy. The "Anti-Pretexting Working Group" is made up of a broad spectrum of ILECs, Wireless Carriers, Cable Operators and a leading CLEC, including: AT&T, Charter, Cingular, Comcast, Cox, Qwest Communications International, Sprint Nextel, Time Warner Cable, Verizon, and XO Communications. The Working Group welcomes new members who wish to sign on to these Best Practices at any time.

Working diligently on a daily basis, these companies are developing an array of best practices and policy proposals designed to prevent unauthorized access to customer call records without unduly inconveniencing or annoying consumers. The attached submission regarding authenticating customers who request call records is the first step in this process; additional measures are being developed and will be shared with the Commission in the near future.

Enclosed with this letter are the Anti-Pretexting Working Group's Best Practices for authenticating consumer customers (hereafter "customers") in order to prevent pretexting of call detail records.

The attached Authentication Best Practices document does not include specific information about the particular data elements used by businesses to authenticate customers; including this information would serve as a roadmap for pretexters and undermine our objective. Instead, it sets out a range of authentication methods that have proved effective to date. The Working Group's efforts on authentication will continue. The Working Group intends to share

W. O. Cuples rec'd
List A B C D E

0 + 4



information regarding new pretexter tactics and new technologies to update the Best Practices as warranted, reporting on its efforts to the Commission.

We are happy to answer any questions the Commission may have regarding the Group's Best Practices thank you for your consideration.

Sincerely,

A handwritten signature in black ink that reads 'Jim Halpert'.

Jim Halpert

Counsel to the Anti-Pretexting Working Group

cc: Michelle Carey, FCC
John Hunter, FCC
Bruce Gottlieb, FCC
Ian Dillner, FCC

Enclosure



**ANTI-PRETEXTING WORKING GROUP
BEST PRACTICES FOR AUTHENTICATING REQUESTS FROM PURPORTED
CUSTOMERS RELATED TO CALL DETAIL RECORDS**

The Anti-Pretexting Working Group is releasing the following Best Practices for authenticating consumer customers (hereafter “customers”) who make sensitive requests related to call detail records and information used to obtain call detail records. This document is the first part of the Anti-Pretexting Working Group Best Practices for preventing “pretexters” from obtaining call detail records data. It balances the need for convenient, efficient customer access to information about the customer’s account with the need to secure call detail records. The Anti-Pretexting Working Group is proposing the Best Practices as a safe harbor by which companies can comply with the Commission’s security requirements for CPNI. The best practices do not apply to other requests, such as requests by law enforcement, requests made pursuant to a subpoena, or otherwise required by law or regulation.

A. WHAT DATA ELEMENTS/ACTIVITIES REQUIRE SECURE AUTHENTICATION TO RELEASE UPON REQUEST?

The Authentication Best Practices set forth in this section are focused on secure authentication for requests for call detail records, changes of address to which call records are sent, and CPNI authentication data that CPNI pretexters attempt to target. The business models of the service providers (telephone companies, wireless carriers, cable operators and others) who follow these Best Practices vary. Depending upon their business, some service providers may implement secure authentication for other requests. Nothing in this document should be interpreted as preventing a service provider from offering secure authentication for other transactions and requests. For example, service providers may employ one or more of the secure authentication methods listed below for customer requests to change service locations or requests that require the disclosure of other sensitive information that is not CPNI.

Service providers who follow the Anti-Pretexting Working Group Best Practices shall employ a secure authentication method appropriate to the context of the sensitive requests (as set forth in subsection C).



For purposes of the Best Practices:

1. The term “call detail record” means a record of a number to which the customer placed a call or from which the customer received a call.

2. The term “sensitive request” means:

- a. A request for call detail record information;
- b. A request to change an address or fax number of record for the account;
- c. A request to establish the passcode, or a request to reset or change the passcode for the account when the customer cannot provide the existing passcode;
- d. A request for a duplicate bill to be sent anywhere except an address of record for the account; and
- e. A request for any data that itself is used as a secure authenticator (e.g. account number information if used as a secure authenticator).

Service providers are not required to securely authenticate a request that any of the above information be delivered to an address or fax number of record for the account.

B. WHEN AND HOW SHOULD CUSTOMERS BE NOTIFIED OF THEIR OPTION TO CHOOSE A VOLUNTARY PASSCODE?

1. How the notice should be presented.

Service providers shall provide customers with clear notice of the customers’ option to secure sensitive requests relating to the customer’s account by means of a secure authentication method. The notice shall be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer. Notice by e-mail should also ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail.



The notice shall be presented to the customer by one or more of the following means, as appropriate for the service provider's business model:

- **Online:** by means of a clear hyperlink on the service provider's Internet home page or the online location where users sign-up for online account access, or by email or text message sent to the email address or wireless text message address of record for the account (if e-mail is used service provider should ensure that the subject line clearly and accurately identifies the subject matter of the e-mail);
- **By phone:** by means of a statement by a customer service representative;
- **By mail:** by means of an insert in, or message on, the customer's bill, or via a separate mailing;
- **In a retail store owned by the service provider:** by means of a notice posted at the retail store or available to a customer who engages in a transaction at a service provider's retail store;
- **Privacy Policy:** clear notice of a customer's option to choose a secure authentication included in the service provider's privacy policy; or
- **On the service provider's service:** by a secure message presented to the customer in a clearly visible location as part of the service that the customer receives from service provider.

2. Contents of the notice.

The notice shall clearly disclose to the customer that the customer has the option to choose to passcode-protect sensitive requests, the requests to which this option applies, and the way(s) that the customer may exercise this option.

3. When notice should be provided.



The customer shall be provided with the notice:

- a. when the customer begins service with the service provider;
- b. when the customer expresses concern to a customer service representative regarding the confidentiality of the customer's account information or requests passcode; and
- c. through notice that is either regularly available to, or is provided periodically (at least annually) to the customer.

4. How the customer may exercise the choice to passcode-protect sensitive data elements.

Customers shall be able to notify the service provider that the customer wishes to choose using a passcode to protect sensitive account information through a one-time request by one or more of the following means:

- phone call to a customer service representative;
- electronically through the service provider's website;
- by an electronic mail or text message to an address specified by the service provider;
- electronically over a secure communication channel of the service provider's network;
- a notarized letter that is mailed to a postal address specified by the service provider; or
- at a retail location owned by the service provider.

The service provider shall authenticate the person making the sensitive request by means of a method set forth in subsection C below before allowing the customer to initiate passcode protection.



C. SECURE AUTHENTICATION METHODS FOR SENSITIVE REQUESTS THROUGH DIFFERENT MEDIA.

Because different communications media raise different authentication challenges and possibilities, the range of secure authentication methods in these Best Practices varies. Service providers should authenticate persons who make sensitive requests for data elements that require secure authentication by means of at least one of the following secure authentication methods appropriate to the context of the request. The secure authenticator should be used in conjunction with whatever other authentication methods that the service provider uses. As technology and security measures evolve, other authentication methods that provide comparable security will be entirely appropriate for service providers to use to fulfill the secure authentication requirements of this section.

1. Online sensitive requests.

a. passcode; or,

b. if the customer cannot provide a passcode:

(1) information on a bill that only the customer and other parties with whom the customer has shared this information are reasonably likely to know;

(2) confirming email, wireless text or postal mail message to an address of record for the account that was established on activation or was reset in accordance with Subsection C. of this document , or phone call to which the recipient responds to authorize the request;

(3) other information about the customer that only the customer is reasonably likely to know; or

(4) by a secure message presented to the customer in a clearly visible location as part of the service that the customer receives from service provider.

2. Sensitive requests over the phone.

a. passcode (if the customer elects to choose passcode authentication);



b. information on a bill that only the customer and other parties with whom the customer has shared this information are reasonably likely to know;

c. other information about the customer that only the customer is reasonably likely to know; or

d. confirmation via email, wireless text or postal mail message to an address of record for the account that was established on activation or was reset in accordance with Subsection C. of this document, or return call to the account phone number on a wireline account or “can be reached at” alternate phone number on a wireless account.

3. Sensitive requests in a retail location owned by the service provider.

a. valid photo identification card or government-issued identification card;

b. passcode (if the customer elects to choose passcode authentication); or

c. other information about the customer that only the customer is reasonably likely to know; or

d. confirmation via email, wireless text or postal mail message to address of record for the account that was established on activation or was reset in accordance with Subsection C. of this document, or return call to the account phone number on a wireline account or “can be reached at” alternate phone number on a wireless account.