



DLA Piper US LLP
1200 Nineteenth Street, NW, Suite 700
Washington, DC 20036-2430
www.dlapiper.com

Jim Halpert
jim.halpert@dlapiper.com
T 202.861.3938
F 202.689.7502

November 10, 2006

VIA HAND AND ELECTRONIC DELIVERY

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

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:

On November 9, 2006, the Anti-Pretexting Working Group ("Group")¹ met with Bill Dever, Adam Kirschenbaum, Tim Stelzig and Cindy Spiers of the Wireline Competition Bureau. The Group includes a broad spectrum of ILECs, Wireless Carriers, Cable Operators and a major CLEC ("service providers").

We discussed: (1) the Group's authentication best practices filed in the *ex parte* docket last week; (2) the scope of account activity that should be subject to secure authentication; (3) the Group's efforts to develop best practices on notifying customers regarding acts of pretexting; (4) the Group's concerns regarding avoiding providing a roadmap to pretexters regarding security measures used to prevent pretexting; (5) the different authentication practices and policies that govern residential customer records versus business customer records; and (6) verifying the validity of online accounts.

Consistent with the Commission's *ex parte* rules, please associate this letter, which is being filed electronically, with the above-captioned docket. Please contact me you have any questions related to this filing.

Sincerely,

Jim Halpert
Counsel to the Anti-Pretexting Working Group

cc: Bill Dever, FCC
Adam Kirschenbaum, FCC
Tim Stelzig, FCC
Cindy Spiers, FCC

Enclosure

¹ The Anti-Pretexting Working Group was represented by Jim Halpert and David Lieber, DLA Piper US LLP, counsel to the Working Group. Among the participating companies, the following companies were present at the meeting: Donna Epps and Josh Swift, Verizon; Lisa Youngers, XO Communications; Lynn Star, Qwest; and Anisa Latif, AT&T.

STATE SECURITY BREACH HARM STANDARDS

Arkansas: "Notification under this section is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers."

Colorado: "The individual or the commercial entity shall give notice as soon as possible to the affected Colorado resident unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur."

Connecticut: "Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."

Indiana: Notification is required where "the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception (as defined in IC 35-45-5-3.5), identity theft, or fraud affecting the Indiana resident."

Kansas: "Security breach" means "the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer."

Louisiana: "Notification under this title is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers."

Montana: "Breach of the security of the data system" means "unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident."

New Jersey: "Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible."

Ohio: Notification is required "if the access and acquisition [of computerized data containing personal information] by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident."

Rhode Island: Notification is required for "any breach of the security of the system which poses a significant risk of identity theft following discovery or notification of the breach...."

Utah: "If an investigation . . . reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident."

Washington: "A person or business under this section shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity."

Wisconsin: Notification is not required if the "acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."