Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20054

Petition for Rulemaking to Enhance	)	
Security and Authentication Standards	)	CC Docket No. 96-115
For Access to Customer Proprietary	)	RM No. 11277
Network Information	)	

COMMENTS OF SBC COMMUNICATIONS INC.

SBC Communications Inc. ("SBC") on behalf of its local exchange carrier affiliates, hereby submits these comments in response to the Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC").[1]

SBC shares EPIC's interest in protecting customer information. Protecting the privacy of customer communications and records is a critical component of customer care, and lies at the heart of SBC's business. In today's intensely and increasingly competitive environment, carriers must take care of their customers if they are to succeed. In addition, SBC naturally desires to protect itself and its customers from potential harm that could be caused by fraudsters. SBC thus has an ongoing incentive to take all necessary steps to safeguard customer information, and has and continues to proactively do so.

SBC takes its obligation to comply with customer proprietary network information ("CPNI") and state privacy laws seriously, and in that regard has devoted numerous resources towards, and implemented varying practices and procedures to, safeguarding the privacy of its customer information. As a general matter, SBC has a Code of Business Conduct ("Code") which requires all employees to comply with all state and federal laws, including CPNI requirements, and with SBC policies regarding the privacy of communications, and the privacy and security of customer records. Employees who fail to meet any of the standards set forth

[1] 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).

therein are subject to disciplinary action, up to and including dismissal. SBC proactively investigates allegations that an employee(s) has breached the Code and, where appropriate, takes disciplinary action and initiates corrective action to prevent future recurrences. SBC has also charged several organizations with protecting its servers, systems, customer communications and records, including Privacy, Asset Protection, Corporate Information Security and Corporate Fraud.

Turning to the specifics, to prevent employee misuse or improper disclosure of CPNI, SBC limits access to CPNI to those employees who need such access to perform their job functions, and trains these employees on the proper use and protection of CPNI. To protect the security of its servers and the information contained therein, SBC requires employees and customers to provide user names and passwords to access sensitive data, and uses industry standard encryption methods to protect data transmission. To prevent unauthorized access to CPNI via the Internet, SBC verifies customer requests to access CPNI on-line to ensure that the customer, and not a third party, in fact registered for the on-line service. Additionally, SBC works closely with customers and law enforcement to bring fraudsters to justice and, in that vein, assists customers in reporting fraudulent action to the relevant law enforcement entities, and law enforcement in its investigations of alleged criminal fraud.

SBC will continue to dedicate resources to prevent unauthorized access to such customer information. Mandated security measures, however, are not the solution. Fraudsters are inventive and always try to stay one step ahead. As soon as carriers implement mandated security measures, these scammers will immediately try to figure out a way around them. Mandated security measures would likely become obsolete rather quickly, and be ineffective long-term. Further, because carriers experience varying types of security breaches, any one-size-fits-all approach would not fix the problem for all. Not to mention, implementation of mandated security measures is costly, and customers ultimately would have to bear these expenses. Given these realities, carriers remain in the best position to determine the most

appropriate, efficient, and cost-effective method of safeguarding their customers' information, and thus must retain the flexibility to both anticipate and respond to fraudulent activity.

Moreover, since telecommunications carriers are not the perpetrators of the alleged misconduct, any remedy directed at carriers, rather than the wrongdoers, would not stem the criminal activity EPIC alleges. Until existing laws are enforced and strengthened, these wrongdoers will continue to engage in this activity.

SBC does not believe a rulemaking proceeding is necessary or warranted at this time. SBC is proactively taking the necessary precautions to safeguard its customers' information and to address any security breach or unauthorized access or disclosure of such information. A rulemaking proceeding at this time could only lead to the imposition of inflexible security rules that would not stem the fraudulent activity, but would impose significant costs on carriers and ultimately consumers. Rather, SBC supports state and federal law enforcement agencies taking action to enforce existing laws and, where appropriate, to strengthen the penalties and consequences associated with fraudulent access to customer information.

Respectfully submitted,

SBC Communications Inc.

/s/ Davida M. Grant
Davida M. Grant
Gary L. Phillips
Paul K. Mancini

SBC Communications Inc.
1401 I Street, NW
Suite 1100
Washington, DC 20005

(202) 326-8903- telephone
(202) 408-8745 - fax

October 31, 2005

Its Attorneys