

Bureau of Regulatory Review Workplan

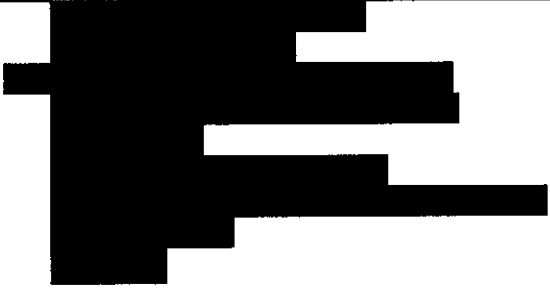
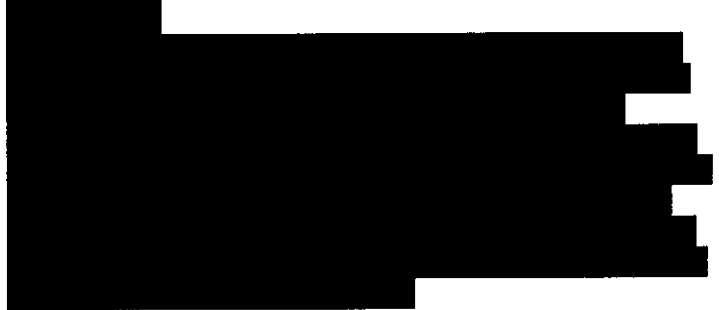

Review of ILEC Customer Data Security

MANAGEMENT OVERSIGHT

Item	Question / Task	Audit Hours	Standard	Audit Notes	Finding
<p>A</p> <p>CMP </p> <p>COM</p> <p>CTR</p> <p>ECR</p> <p>GCL</p> <p>OPC</p> <p>FOA</p> <p>SCR</p> <p>SSP</p> <p>SLC</p>	<p>Does company management have a clear understanding that information security is a management responsibility?</p> <p>(DR-1 Q 1)</p>		<p>Appropriate written policies and procedures should exist.</p> <p>These policies and procedures should serve as a 'recipe' to guide all activities advancing company goals and objectives relevant to network and sensitive customer information security.</p> <p>Policies and procedures should be consistent with best industry practices for information security.</p> <p>Policies and procedures relevant to information security should be regularly reviewed and updated as needed.</p> <p>Employee and corporate compliance with policies and procedures should be regularly reviewed and verified by management.</p> <p>The company should have specific policies and procedures relevant to network and information security.</p> <p>Policies and procedures should be proper, suitable and relevant.</p> <p>Policies and procedures as they relate to data security should define the end result(s) sought.</p> <p>Policies and procedures should be specific, measurable, and support the ILEC vision of data security.</p> <p>Policies and procedures should focus</p>	<p>AT&T: DR-1 responses make it clear that AT&T has a clear understanding of management's responsibility re information security. Policies and procedures exist and are comparable to those of other industry leaders. Many are new due to the recent merger of BellSouth with AT&T. Policies and procedures are specific, reviewed, supervised by IT and management, and require regular renewal by employees. Security policies are compatible with ISO/IEC 27000 series, the Alliance for Telecommunications Industry Solutions (ATIS) T1M1 Security Standards, and Network Reliability and Interoperability (NRIC) security best practices.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	

Bureau of Regulatory Review Workplan

Review of ILEC Customer Data Security

				
<p style="text-align: center;">C</p>	<p>Has the company assessed the appropriateness of the information collected from customers?</p> <p>(DR-1, Q 13)</p>	<p>Management should regularly assess risks associated with the acquisition, processing, storage, security, and inside/outside threats associated with sensitive customer data.</p> <p>Management should evaluate risks and develop a model/procedures to reduce and overcome these risks.</p> <p>Management should evaluate how risk(s) impact and inhibit overall performance.</p>	<p>AT&T: AT&T management actively assesses risk of all sorts, including security, using an iterative risk assessment process. The company also has policies and standards on how to properly handle, collect, safeguard, store, and destroy sensitive customer information. Management reviewed and approved the information collected from customers. Security considerations are integral to the Software Development Lifecycle (SLDC). AT&T uses a Risk Identification, Assessment, Analysis, and Mitigation process. Final risk rating and a mitigation plan is reviewed and approved by the Chief Security Office Risk Evaluation Committee (CSO REC) along with the managers of the business unit which "owns" the risk. It is then tracked until closure by both parties.</p>  	

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

D	Does the company adequately limit the use and disclosure of customers' personal information?		<p>Management should develop internal controls based on the risks associated with system integrity and operational procedures.</p> <p>Sensitive information security protection methodologies should be both active and passive.</p> <p>Controls should allow the company to reduce exposure to potential loss of information.</p> <p>Management should continually monitor compliance with data security initiatives.</p> <p>ILECs should document lapses in its security initiatives. Results should be provided to management in a measurable format.</p>	<p>AT&T: AT&T uses access controls based on the principle of "least privilege" and "need to know". IT regularly reviews (often in real time) internal controls and system integrity through automated processes. Anomalies are automatically identified. A full range of IPS and IDS protocols are employed to secure customer information. Training, policies, and procedures are in place to make employees aware of their responsibilities. Disciplinary policies and procedures are clear and comprehensive as they pertain to data security misconduct.</p>	<p>AT&T Masking does not include SSAN.</p>
E	Do any employees have access to customers' personal information at off-site facilities? (DR-1, Q 16)		<p>Does the company have a work-from-home program for customer service reps or others?</p> <p>The company should have high, defined selection criteria for work-at-home employees.</p>	<p>AT&T: Yes, select employees have access to the system from offsite locations. This requires the use of Virtual Private Network (VPN) software and a two-factor authentication such as a one-time password generator.</p>	<p>AT&T 2,319 workers have full access to SSAN and banking info.</p>

Bureau of Regulatory Review Workplan
Review of HEC Customer Data Security

F	<p>What controls has the company put in place for remote access of sensitive customer personal information?</p> <p>(DR 1, Q 1) (DR-1, Q 16)</p>	<p>What control measures are in place to secure:</p> <ul style="list-style-type: none"> o Work area access o Hardware security o Network security o Software security <p>The company should clearly designate responsibility for data management.</p> <p>Has the company created a position whose sole responsibility is data security?</p> <p>The company should establish a synergistic defense using active intrusion detection systems (IDS) and passive intrusion protection systems (IPS).</p> <p>Encryption certificates levels should be in keeping with industry standards (128-bit is the optimum).</p>	<p>AT&T:</p> <p>Access requires the use of Virtual Private Network (VPN) software and a two-factor authentication such as a one-time password generator. VPN communications are encrypted during transmission. Once into the system, the accessing employee has normal access and the full complement of hardware, software, and system security measures. AT&T has a Vice President/Chief Security Officer, responsible for overall Data Security. AT&T uses a meshed IPS/IDS defense.</p>		

INFORMATION TECHNOLOGY (IT) CONTROLS

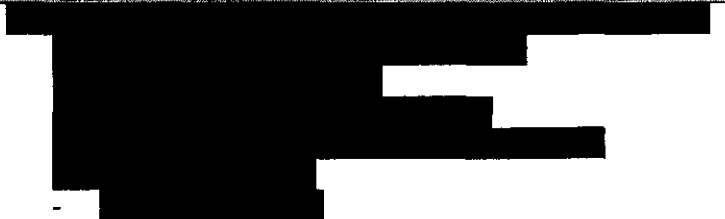


G	<p>Has the company established an appropriate data security management function?</p>	<p>The company should use a layered network defense including elements such as:</p> <ul style="list-style-type: none"> o Firewalls o IDS / IPS o Internet content filtering o Instant messaging (IM) protection 	<p>AT&T:</p> <p>AT&T employs a fully integrated, automated, set of IPS and IDS defenses for system security. The company has established the position of Vice President/Chief Security Officer. He or she is responsible for overall data security. Immediately subordinate is the Director of Security Planning and</p>		
---	--	---	---	--	--

Bureau of Regulatory Review Workplan

Review of ILEC Customer Data Security

<p>(DR-1, Q-1)</p>	<ul style="list-style-type: none">○ Routine scans of perimeter devices○ Virus protection○ Vulnerability assessment (BIGFIX)○ Vulnerability remediation <p>Individual desktop workstations and servers should be protected by elements including:</p> <ul style="list-style-type: none">○ Standardized security configurations○ Standardized security settings○ Centrally managed upgrades○ Concept of "least privilege"○ Regularly review access <p>IT responsibilities may include:</p> <ul style="list-style-type: none">○ Formal development life cycle○ Developer training for security coding○ Real time scanning of applications○ Change process for applications○ Change process for infrastructure○ Creating security-specific policies○ Creating security-specific procedures○ Conducting internal audits○ Coordinating external audits	<p>Engineering. He or she manages the Exec Director of Enterprise Security Infrastructure, Exec Director of Identity and Access Management, and Exec Director of Security Policy and Compliance. Subordinate to those ExecDirectors are various directors, including:</p> <ul style="list-style-type: none">- Dir-Security Information Management- Dir-Distributed Security Solutions- Dir-Enterprise Network Security- Dir-Network Security Solutions- Dir-IAM Operations- Dir-IAM Development & Production- Dir-PCI, SOX, and Audits- Dir-Security Compliance Processes <p>An AsstVP for Security, Technology & Services has responsibility for the ExecDirector of Security Services and Engineering, Threat Management, and Government Select Security Programs. Subordinates to them includes:</p> <ul style="list-style-type: none">- Dir-Advanced Security Research- Dir-Portal Development & Integration- Dir-Premises Security Services- Dir-Threat Management Platform- Dir-Custom Software Solutions <p>[REDACTED]</p> <p>[REDACTED]</p>	
--------------------	---	--	--

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

					
H	<p>Does the company limit physical access to customer information data resources through access authorization procedures, monitoring devices, and alarm systems?</p> <p>(DR-1, Q 7-10, 12, 15, 16)</p>	<p>Personnel access to facilities handling sensitive information should be controlled, monitored and regularly tested.</p> <p>Control methodologies may include:</p> <ul style="list-style-type: none"> o Remote or interior location o Tightly limiting visitors o Escorting visitors o Fencing o Video surveillance o Security gates o Magnetic key entry o Cipher locks on exterior doors o Guards o Windowless construction o Signal attenuating walls o Regular penetration testing 	<p>AT&T:</p> <p>AT&T controls access to facilities in the same manner as to applications – the principles of “least privilege” and “need to know”. Training, policies, and procedures are in place to make employees aware of their responsibilities regarding proper and authorized access to facilities. Disciplinary policies and procedures are in place as they pertain to facility security measures and violations of policy. Specific physical protocols to be viewed during onsite visit to Alpharetta, GA.</p> <p></p> <p></p>		
I	<p>Does the company restrict access to customer information related software functions, data and programs?</p>	<p>The company should use a form of “least privilege” and “need to know” when allocating access rights to employees.</p> <p>Employees should receive access to only those areas necessary for job accomplishment.</p>	<p>AT&T:</p> <p>AT&T uses “least privilege” and “need to know”. Training, policies, and procedures are up to date. A variety of methodologies are used (print, interactive online, multimedia, classroom) to teach employees about proper and authorized access. Disciplinary policies and procedures exist relevant to access policies and procedures. IT regularly and automatically</p>	<p>AT&T</p> <p>Masking does not include SSAN.</p>	

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

	<p>(DR-1, Q 7-10, 12, 15, 16)</p>		<p>IT should regularly screen access.</p> <p>IT should regularly report to company management the results of access screening.</p> <p>Sensitive customer information should be masked</p>	<p>screens access, generating anomaly reports.</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>J</p>	<p>Does the company monitor software security activity and produce appropriate management reports?</p> <p>(DR-1, Q 10, 12, 13)</p>		<p>IT should regularly screen access.</p> <p>IT should regularly report to company management the results of access screening.</p> <p>ILECs should be conducting internal and/or external audits of sensitive data security.</p>	<p>AT&T:</p> <p>IT regularly and automatically screens access, generating anomaly reports. Five information security related audits were conducted in 2006-2007. AT&T provided lists of scope, controls, findings, and remedial actions for all audits. An audits is planned for 2008 (Privacy of Customer Information), tentatively scheduled to begin May.</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	

Bureau of Regulatory Review Workplan
Review of TLEC Customer Data Security

--	--	--	--	--	--

USER AWARENESS AND TRAINING

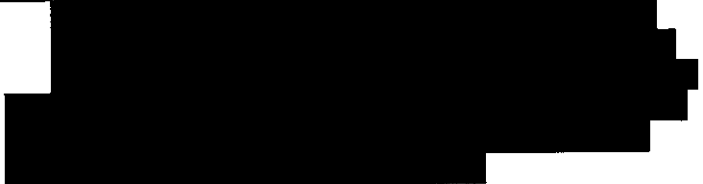


K	<p>Does the company have adequate privacy and data security policies and procedures? (DR-1, Q 2)</p>	<p>Appropriate written policies and procedures should exist.</p>	<p>AT&T: Written policies exist and the company provided a copy of the <i>AT&T Enterprise Privacy Policy, AT&T Security Policy and Requirements (ASPR), and the AT&T Code of Business Conduct.</i> All policies and procedures appear relevant and geared toward industry best practices. The merger of BellSouth and AT&T allowed the new enterprise to refocus on this critical documents as well as the policies and procedures that dovetail with them. This allowed review, revision and retraining.</p>
		<p>These policies and procedures should serve as a 'recipe' to guide all activities advancing company goals and objectives relevant to network and sensitive customer information security.</p> <p>Policies and procedures should be consistent with best industry practices for information security.</p> <p>Policies and procedures relevant to <i>information security</i> should be regularly reviewed and updated as needed.</p> <p>Employee and corporate compliance with policies and procedures should be regularly reviewed and verified by management.</p> <p>The company should have specific policies and procedures relevant to network and information security.</p> <p>Policies and procedures should be proper, suitable and relevant.</p> <p>Policies and procedures as they relate to data</p>	

Bureau of Regulatory Review Workplan

Review of ILEC Customer Data Security

		<p>security should define the end result(s) sought.</p> <p>Policies and procedures should be specific, measurable, and support the ILEC vision of data security.</p> <p>Policies and procedures should focus employees to achieve a specific outcomes relevant to security of sensitive customer information.</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
<p>L</p>	<p>Are company employees properly trained on privacy and data security policies?</p> <p>(DR-1, Q 18)</p>	<p>ILECs should have adequate training materials to instruct its employees.</p> <p>Training materials should detail specific job functions and steps to protect sensitive customer information.</p> <p>Materials should be detailed and easily accessible to all employees.</p> <p>ILECs should verify that each employee completes all necessary training.</p> <p>ILECs should have a Code of Ethics for employees.</p> <p>This code should include a statement concerning protecting customer personal and sensitive information.</p> <p>Employees regularly acknowledge the Code of Ethics.</p>	<p>AT&T:</p> <p>The BellSouth merger into AT&T allowed the new AT&T to perform a comprehensive relook-rewrite of training programs, policies and procedures for the new company going forward. Reviews, revisions and retraining were undertaken as a consequence of the merger. Written policies that the company provided included the <i>AT&T Enterprise Privacy Policy</i>, <i>AT&T Security Policy and Requirements (ASPR)</i>, and the <i>AT&T Code of Business Conduct</i>. Materials are new or newly revised, easily accessible for all employees, and geared toward industry best practices.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

					
M	<p>Does the company have policies and procedures in place which address penalties for violations of privacy or data security policies?</p> <p>(DR-1, Q 2)</p>		<p>Company should have written disciplinary guidelines for violations of company policies relevant to data security and/or privacy.</p> <p>Policies should be well known throughout the company, acknowledged by all employees, and regularly reviewed with refresher training.</p> <p>Violations of company policy and procedures regarding protection of customer sensitive information should be addressed responsively by management.</p>	<p>AT&T: The <i>AT&T Enterprise Privacy Policy</i> stipulates that every employee's responsibility for securing sensitive customer data. It requires that every employee follow applicable laws, rules, regulations, court and/or commission order that applies to AT&T at all times. In addition, the <i>AT&T Security Policy and Requirements (ASPR)</i>, mandates that all employee and non-employee personnel performing work on behalf of AT&T are fully accountable (and subject to disciplinary actions, up to and including dismissal) for unauthorized access, interception, disclosure, misuse, modification, destruction, theft, or impairment. Although there are many other security-related publications within AT&T, the ASPR is <u>the</u> document. Every AT&T security-related document is available to each employee on the company intranet at http://cso.att.com</p>  	

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

OUTSOURCING CONTROLS

N	<p>Does the company provide third parties with access to customer personal or banking information?</p> <p>(DR-1, Q 19, 21)</p>	<p>The company should have standardized written procedures for screening third party vendors.</p> <p>Third party employees with access to ILEC network and sensitive customer data should pass security checks similar to ILEC company employees.</p> <p>Network and/or controlled access facility use by third party vendors should be subjected to "least privilege" and "need to know" criteria.</p> <p>Network and/or controlled access facility privileges initiated only when and to the exact extent required.</p> <p>When no longer needed, network and/or controlled access facility privileges terminated immediately.</p> <p>Third party network and/or controlled access facility privileges should be routinely and regularly scanned/screened while in effect.</p>	<p>AT&T: Yes, AT&T individually determines and authorizes both access, the level of access, and those third party individuals who are granted it on a case-by-case basis. The AT&T business unit responsible for managing the services provided by a third party has responsibility for this process and recommendations governing such access.</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	[REDACTED]
O	<p>What controls has the company put in place to prevent disclosure of customers' personal information</p>	<p>Controls for third parties may include:</p> <ul style="list-style-type: none"> o Training to company standards o Confidentiality agreements o Formal process to determine access o Validation of access requests 	<p>AT&T: All third party employees must sign a non-disclosure agreement or be covered by a similar instrument signed by the third party representatives. Third party individuals must agree to follow all security directives of the AT&T CSO and those written policies /</p>	[REDACTED]

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

	<p>by third parties? (DR-1, Q 21)</p>		<ul style="list-style-type: none"> o Keeping access logs o Access reports o Supervisory oversight o Right to audit o On-site survey to evaluate vendor ability to protect sensitive data 	<p>procedures of the ASPR. Background checks are required. Third party employees are required to read and acknowledge the same privacy policies and ethics standards as AT&T employees.</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>
--	--	--	---	---	-------------------

AUDITING CONTROLS

<p>P</p>	<p>Does the company possess, or have access to, competent auditing resources to evaluate information security and associated risks? (DR-1, Q 24)</p>		<p>Audits should be used to evaluate the effectiveness of protection for overall system integrity and sensitive customer data</p> <p>Audits and studies should reveal problem areas and provide detail on level of severity of the problem. .</p> <p>Audit findings should be properly addressed by management in the form of operational changes.</p> <p>Follow-up audits of remedial efforts may be</p>	<p><u>AT&T:</u> Yes. AT&T has two processes for assessing security compliance and risks associated with security. These are:</p> <ul style="list-style-type: none"> - Internal Audits - Security Evaluation Prgm (SEP) <p>Internal audits are conducted by AT&T Audit Services. SEP is conducted under the direction of the CSO. Both are focused on vulnerabilities, discovery, tracking of compliance with ASPR requirements and reporting via scorecards. Potential weaknesses are identified and each business unit works with the SEP team to develop resolution, remediation and risk mitigation strategies. Other scorecards track results; these are distributed to business unit contacts monthly and vice-presidents quarterly. Five</p>	<p>[REDACTED]</p>
----------	---	--	---	--	-------------------

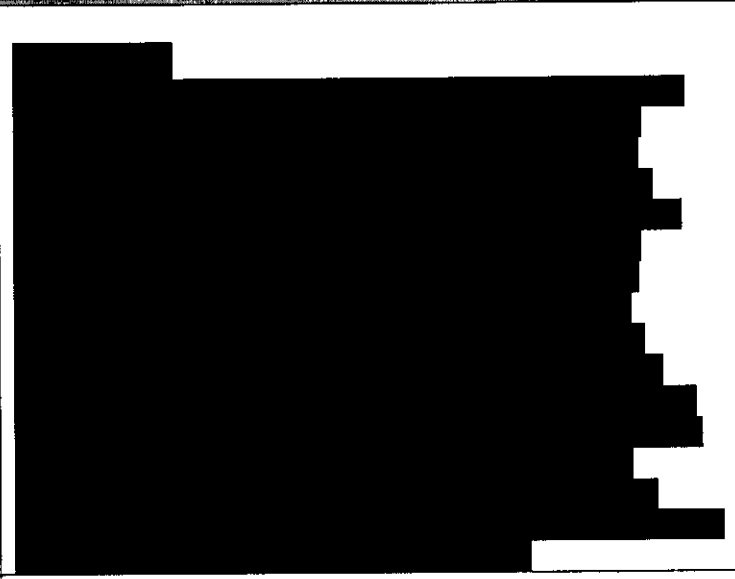

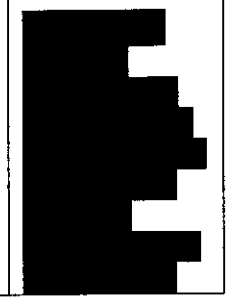
Bureau of Regulatory Review Workplan

Review of IEEC Customer Data Security

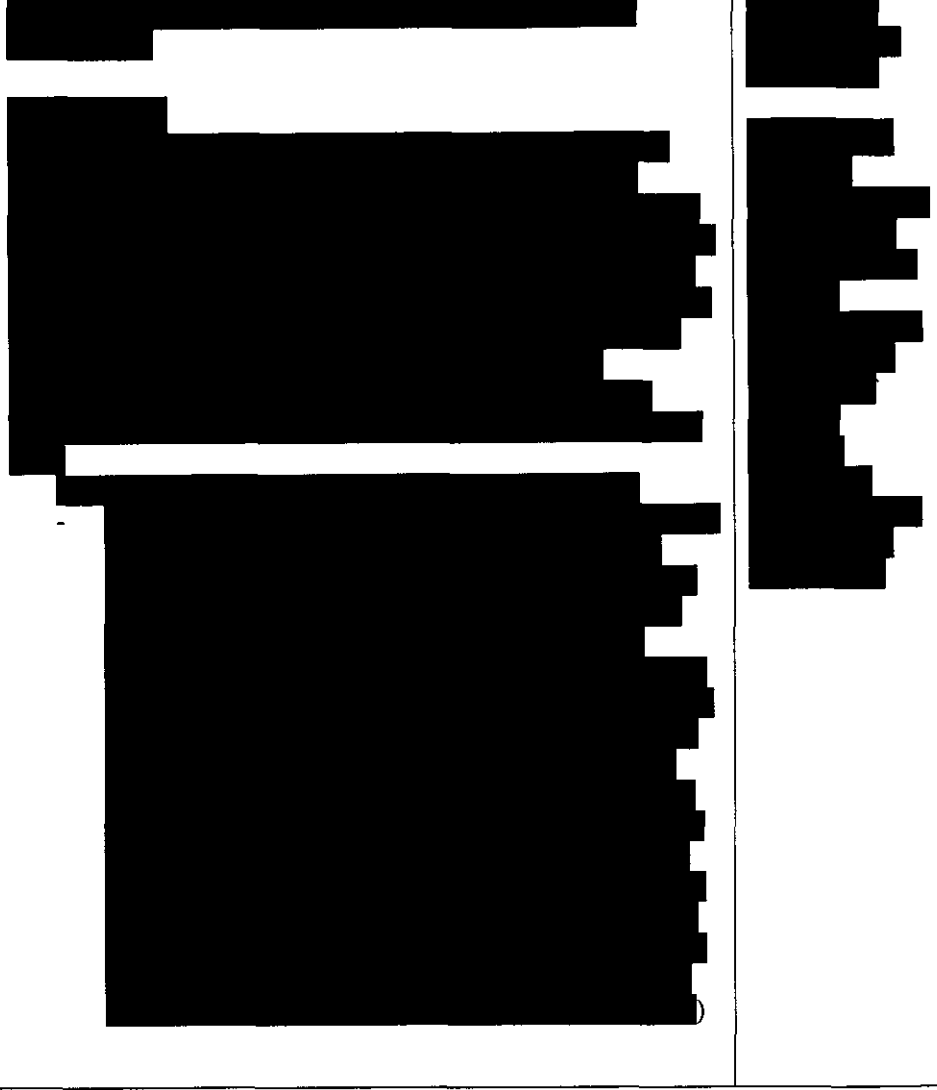
		<p>required.</p>	<p>information security related audits were conducted in 2006-2007. AT&T provided lists of scope, controls, findings, and remedial actions for all audits. An audits is planned for 2008 (Privacy of Customer Information), tentatively scheduled to begin May.</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
<p>Q</p>	<p>Does the company periodically assess the organization's information security practices?</p> <p>(DR-1, Q 2, 6, 22, 24, 25)</p>	<p>Company policies and procedures relevant to information security should be regularly reviewed and updated as needed.</p> <p>Employee and corporate compliance with policies and procedures should be regularly reviewed and verified by management.</p> <p>Regular internal and external audits should be an integral part of the company's strategy to assess network and information security.</p>	<p>AT&T: Yes. The ASPR (Chap 2.8) defines security assessments as intrusion testing, sweeps, profiles, penetration testing, ethical hacking, auditing, and vulnerability analysis. Security analysis of AT&T networks or computers is done in-house; external vendors or consultants are expressly prohibited unless written approval is obtained from the CSO. Chapter 2.7 requires that application, system and network administrators must perform self-reviews at least annually. Reviews must be carried out using the CSO prescribed tools, checklists and procedures. The AT&T CSO, internal Auditing and other security organizations may also conduct periodic (but without a prescribed time interval) formal assessments and audits to identify vulnerabilities, existing safeguards, and recommended additional safeguards. These formal security assessment do not supersede the need for administrators to perform annual self-reviews.</p> <p>[REDACTED]</p>	<p>AT&T (Possible?) Does lack of outside scrutiny for security assessments lead to laxness?</p> <p>[REDACTED]</p>

Bureau of Regulatory Review Workplan


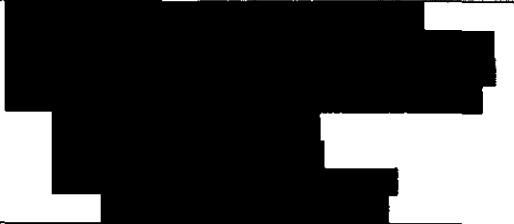


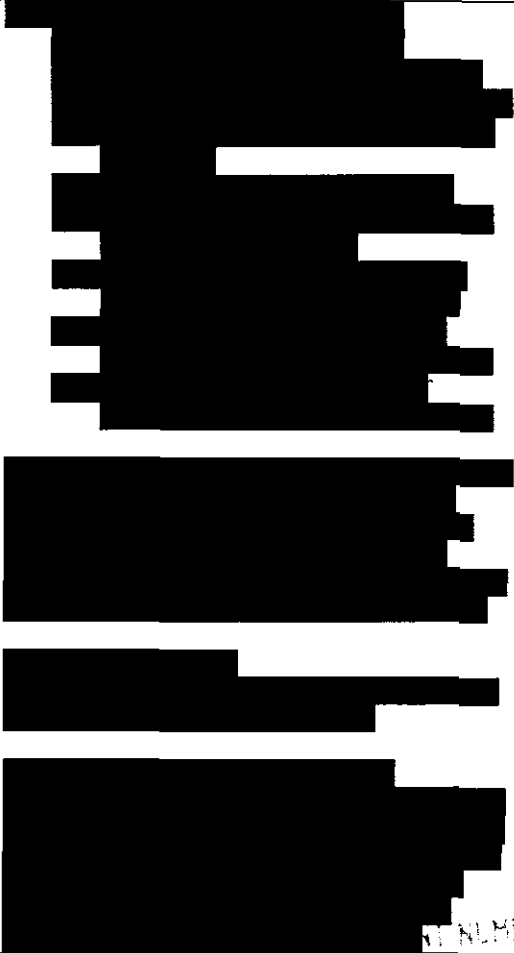

Review of ILEG Customer Data Security

				
R	<p>Has management provided assurance that information security breaches and conditions that might represent a threat to the organization will be promptly made known to appropriate corporate and IT management?</p> <p>(DR-1, Q 10, 22, 23, 25)</p>	<p>The company should have procedures in place to report all threats and security breaches.</p> <p>Threats and breaches should be reported:</p> <ul style="list-style-type: none"> o Quickly o To those responsible internally o To those external agencies as required by regulation or statute <p>The company should expeditiously:</p> <ul style="list-style-type: none"> o Have an operations contingency plan o Alert responsible employees o Secure the breach o Mitigate the threat / vulnerability o Tightly control access to the area o Quantify the compromise o Report internally o Report externally, if required o Alert customers o Repair damage o Devise network defense solution(s) 	<p>AT&T: Yes. The ASPR outlines appropriate contingency actions upon discovery of a breach. AT&T listed incidents of breach and theft:</p> <ul style="list-style-type: none"> - 2005: Five computers were stolen; none were reported recovered. None contained sensitive information. There were 7 claims of unauthorized access. One was substantiated by internal investigators. Disciplinary action followed. None of the cases involved credit card information. - 2006: Eleven computers were stolen; two were recovered. None contained sensitive information. There were 6 allegations of unauthorized access. One was substantiated by the investigation. The responsible employee was disciplined. None of the unsubstantiated cases involved credit card information. The substantiated case was an unauthorized family member accessing customer account information. 	<p>AT&T (Possible) 2005: Was SSAN involved? 2006: Was SSAN involved? Was credit card info compromised?</p> 

Bureau of Regulatory Review Workplan
Review of ILEC Customer Data Security

				
--	--	--	--	--

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>1. Please provide a current company organizational chart depicting work units, job positions and names of personnel responsible for administering customer information security.</p>	<p>Provided a list of personnel responsible for operational, physical, and data security. Prefaced by a note "At AT&T, every person is responsible for maintaining the security of customer information. [. . .] we have provided a copy of the organization chart for our security organization that is primarily involved in assisting the company work units."</p>			 <p>AT&T provided a list but does not have an organizational chart.</p>
<p>2. Please provide copies of:</p> <p>a. Company privacy policies relevant to customer data security and the protection of sensitive customer information.</p> <p>b. Employee Code of Ethics for data security and the protection of sensitive customer information.</p> <p>c. Company disciplinary policies and procedures which specifically address violations of customer data privacy and security protocols.</p>	<p>a. Provided their privacy policies (<i>ATT Enterprise Privacy Policy</i>, dtd 6/16/06, <i>ATT Information Security Policy</i>, dtd 7/01/07, <i>ATT Security Policy and Requirements -ASPR ver 2.1 dtd 11/01/07</i>, and <i>AT&T Information Classification and Protection Standards ver 2.1 dtd 11/01/07</i>). Also provided was the universal company privacy document, <i>AT&T Security Policy requirements (ASPR)</i>, ver 2.0, dtd July 1, 2007. AT&T collects name, address, email address, billing, payment, usage, credit and transactional information. They do not provide personal information to third parties for marketing purposes without customer consent. AT&T does, where permitted or required by law, provide information to third parties (e.g. credit bureaus or collection agencies) They reserve the right to provide such information in order to enforce their own right to payment for services or to protect AT&T property. They will also furnish such information without consent to comply with court orders, subpoenas or other legal or regulatory requirements. Names, numbers, and addresses of customers who have a 'non-listed' number will not be available in AT&T directories but will be publicly available through directory assistance and provided to unaffiliated directory assistance providers over whom AT&T exercises no control.</p> <p>b. In the <i>AT&T Code of Business Conduct</i> provided. Both it and <i>ATT Enterprise Privacy Policy</i> State clearly that it is every employee's responsibility for customer data security. The protection of customer sensitive data and the prohibition to allow unauthorized access, alter or allow alteration, disclose or allow disclosure, and destroy or allow destruction of such data is clearly articulated.</p>			

NUMBER-DAT
 04822 JUN-5 8
 FPSC-COMMISSION CLEAR

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
	<p>c. IAW the <i>AT&T Code of Business Conduct</i>, all employees are subject to the provisions and adverse administrative action ranging from simple counseling, remedial training, to complete dismissal (even for a first offense). Criminal action is possible.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	
<p>3. Please list all references to federal, state, or local rules, and regulations relating to customer data security with which the company must comply.</p>	<p>FEDERAL</p> <ul style="list-style-type: none"> - The Child Online Privacy Protection Act - FTC's COPPA Regulation - FTC Commentary on the FCRA - Section 222 of the Federal Communications Act (47 U.S.C. § 222) - The Fair Credit Reporting Act - FCC's CPNI Rules - FCC's <u>Final Rules</u> on Caller ID - Fair Debt Collections Practices Act - The Federal Trade Commission Act <p>FLORIDA</p> <ul style="list-style-type: none"> - FL Stat. Ann.817.5681 et. seq. requiring notice to consumers on breach of security, confidentiality, or integrity of computerized, unencrypted personal information held by any person doing business in the state. - FL Stat. §364.24 Employees of telecom companies must not intentionally disclose customer account records, contents, or substance of any message, communication sent, received, or heard to any party other than 	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>Check AT&T [REDACTED] awareness of requirements for</p> <p>Florida laws:</p> <ul style="list-style-type: none"> - Florida Public Records Act - Florida Common Law Right to Privacy <p>Federal laws:</p> <ul style="list-style-type: none"> - Fair and Accurate Credit Transaction Act - Freedom of Information Act <p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>4. Please provide any data security industry best practices and standards to which the company adheres.</p>	<p>the customer without consent.</p> <p>AT&T data security policies have been developed over many years in parallel with the development of industry best practices and standards. AT&T has been a leader in providing input to industry best practices and benefited from others involved in this process. While AT&T policies, per se, do not map specifically to any industry best practices, the company asserts that their actions and policies are compatible with the International Standards Organization's (ISO/IEC) 27000 series, Alliance for Telecommunications Industry Solutions (ATIS) Security Standards, and Network Reliability and Interoperability (NRIC) security best practices.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	
<p>5. a. Please identify the information collected from a new customer when opening an account.</p> <p>b. Has management assessed the specific need(s) for and use of the personal information collected from customers? Please explain.</p>	<p>a. AT&T collects:</p> <ul style="list-style-type: none"> - NAME - ADDRESS - SOCIAL SECURITY NUMBER - Customer initiates a PASSWORD or SECRET CODE that is placed on the account to protect against unauthorized individuals receiving, accessing, or changing sensitive customer account information. - PLACE OF EMPLOYMENT - CONTACT NUMBER other than the established AT&T number - AUTHORIZED USERS, other than the customer - CREDIT or DEBIT CARD NUMBER when customer requests automatic payment. This info is also required to complete wireless, DTV, DSL or customer provided equipment sales processing. Such info, once inputted to the system is not seen on CSA's screens. <p>b. Not addressed</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>AT&T: Has AT&T performed any risk management assessments for the information collected?</p> <p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>6. Please provide any risk analysis studies or evaluations performed by company management in the last 24 months that identified the adequacy of internal security controls relevant to sensitive customer information.</p>	<p>Chief Security Office (CSO) Penetration Team conducted active penetration tests against the AT&T Southeast's mainframe systems. They also tested the AT&T Web Hosting systems. Vulnerabilities were identified, assessed, prioritized and remediated. All complete.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>7. Does the company currently use full or partial masking of sensitive customer information?</p> <p>Please describe the masking methodologies employed.</p> <p>a. Is such masking universal or selective across company network applications and software programs? Please explain.</p> <p>b. How many employees currently have full (unmasked) access rights to sensitive customer information?</p>	<p>a. Some sensitive information such as credit card numbers is masked. Other information is not. The average AT&T employee does not have access to billing systems and/or sensitive customer information.</p> <p>b. Credit card numbers are only stored encrypted. Only a few people have access to the decryption algorithm. Billers do not provide users a means to decrypt this information.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>AT&T: Not a finding (yet): During on-site visits, determine if masking is universal or selective and for which items.</p> <p>[REDACTED]</p>
<p>8. Please explain and describe what internal controls exist to ensure the proper handling and security of sensitive customer information.</p>	<p>AT&T policy sets the company guidelines to protect the security of sensitive customer information. See documents provided in response to DR-1, Item 2. AT&T utilizes general mechanized and automatic controls such as requiring an ID and password for</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
	individual access to customer information. See response to DR-1, Item 12 also. "Least privilege" and a business "need to know" govern access rights.	[REDACTED]	[REDACTED]	
<p>9. Does the company employ a 'defense in depth' strategy for data security, using both intrusion detection systems (IDS) and intrusion prevention systems (IPS) to safeguard sensitive information? Please explain.</p>	<p>Yes, AT&T employs a defense in depth strategy to protect customer sensitive information. The use both IDS and IPS technologies to prevent and detect intrusion activity. Their systems are regularly monitored and updated frequently. Their systems comply with the latest technologies available. Detection and intrusion prevention hardware/software is based on threat information and evaluations from a variety of sources both internal and external. Controls are monitored 24/7 by the CSO team.</p>	[REDACTED]	[REDACTED]	None. All companies employ defense in depth strategies and industry-standard methodologies for accomplishing it.
<p>10. Please describe any changes or improvements made to the network data security protocols or access policies in the last 24 months.</p>	<p>AT&T contends it is "constantly improving our security infrastructure. Several incremental security solutions have been deployed recently. We are adding firewalls and IPS function to our laptops and desktops as the first priority. Finally, we are consolidating, integrating, and improving tools that support our Identity Management processes." AT&T asserts it has enhanced security measures for customer-initiated access to account data. Enhanced access channels include online, in call centers, Interactive Voice Response (IVR) systems and physical stores. Enhancements are to meet the new FCC privacy regulations that took effect 12/10/07. See http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf See <i>AT&T Customer Security Standards</i>, ver 1.02, dtd 2/1/08, provided as an attachment.</p>	[REDACTED]	[REDACTED]	<p>[REDACTED]</p> <p>For AT&T: Det'm a timeline for their improvements (e.g. new firewalls, etc)</p>
<p>11.</p>	AT&T gets announcements of security patches from a	[REDACTED]	[REDACTED]	[REDACTED]

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>Please describe and provide an example timeline for the processes associated with the receipt, validation and installation of security patches.</p>	<p>variety of industry sources including vendor websites, public information, CERT/CC, US-CERT, and AT&T Internet Protect. They are analyzed for applicability to AT&T systems and their potential impact on those systems. They are then assigned a Threat Rating which describes the potential threat of exposure or compromise if the patch is not used or not expedited. By policy, patching 'windows' at AT&T cannot exceed 60 days and may be shortened based on criticality of the vulnerability or the system itself. If the patch is to be installed, it is verified and validated (offline). If problems arise in an environment or application, operations and security organizations internal to AT&T review possibilities for controls or other mitigations to reduce risk, or accept risk as unavoidable due to business need. If the patch passes all validations, it is applied using standardized tools within the appropriate timeframe.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>12. Does Information Technology:</p> <p>a. Restrict employee access to customer information related software functions, data, and programs? Please explain.</p> <p>b. Monitor and employee access to sensitive customer information? Please describe; explain protocols and procedures.</p> <p>c. Produce regular management reports detailing employee access to sensitive customer information? If so, please provide an example of all such reports.</p>	<p>a. ID and password required for all individuals to access customer information. Specific permissions (authorizations) are mandatory. "Least privilege" applies. Based on role and business function -- the need to know. Levels of access vary between individuals in the same work or Business Unit. This also applies to third parties</p> <p>b. As it relates to billing, AT&T logs all access to customer records in the Customer Records Information System (CRIS). A log entry is automatically created each time customer information is accessed by anyone. The entry indicates who, when, and what activities were performed by the employee.</p> <p>c. AT&T produces regular reports -- <i>Access by User Account</i> ("sample-by-cuid.xls" furnished), <i>Access by Telephone Number</i> (sample-by-tn.xls" furnished)</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>13. Please explain how risks specifically associated with Information Technology</p>	<p>AT&T employs and interactive risk process – Risk ID, Risk Assessment, Risk Analysis and Risk Mitigation. Risks may be ID's by vulnerability scanning, audits,</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarg	Verizon	Possible Finding
<p>and relative to the release of sensitive customer information, are identified, evaluated, validated, isolated, prioritized, and corrected.</p>	<p>official compliance requirements of SOX, PCI or HIPAA. Risks are then assessed and rated using three factors – the potential severity of the risk, the cost of impact of the risk, and the likelihood of the risk actually happening. The rating derived determines the frequency and depth of ongoing, future review(s) and assists in deciding the mitigation strategy for the risk. During Risk Analysis the feasibility and cost of different mitigation strategies are evaluated relative to the potential cost impact. A mitigation strategy of Risk Elimination, Risk Reduction, Risk Transfer, or Risk Acceptance is chosen such that the risk is either totally removed, mitigated to an acceptable level, handed off to a third party, or accepted as is. This risk rating and mitigation plan is reviewed and approved/disapproved by the Chief Security Office Risk Evaluation Committee (CSO REC) along with the Business Unit owner. It is then tracked until closure.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	
<p>14. When establishing a new account, is a credit verification service (e.g. Experian) used?</p>	<p>Yes, AT&T uses credit verification services to substantiate a customer's credit rating.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>All companies use industry-leading credit check vendors.</p>
<p>15. Please describe the internal processes and timeline for changing employee access to sensitive customer information for those who terminate employment, retire, or transfer to positions which do not require such access.</p>	<p>Whenever any employee leaves the company, the supervisor must perform the employee exit package (<i>separation_of_employment_guide.pdf</i>) This requires that all access to systems be removed prior to employee exit. Mon – Fri an application runs in real time that denies / deletes access to billing accounts for employees no longer on the payroll. Another real time process collects all system log files from production sites. They are reviewed and each successful log-in is checked against an active employee roster. Exceptions are flagged and sent to the system owner/administrator for action. See <i>Separation of Employment Guide</i>, provided as an attachment.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>16. Describe the virtual security</p>	<p>a. Offsite access requires the use of an approved VPN</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>None. All companies use VPN access</p>

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>safeguards and controls that are in place to protect the network and sensitive customer information for:</p> <p>a. Remote employee access to the network remotely.</p> <p>b. Offsite company facilities.</p>	<p>(Virtual Private Network) software. Remote access also requires two-factor authorization such as a one-time password generator. Details are included in the AT&T security policy entitled <i>General Networks and Remote Access</i>, provided as an attachment.</p> <p>b. EDS uses an approved off-site storage vendor (Iron Mountain) for off-site storage of media. The vendor provides secure transport to and from the storage facility and the secure storage facility itself. See <i>Hardware Technical Support Secure Sync Work Instructions</i>, provided as an attachment.</p>	<p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>controls from off-site.</p>
<p>17.</p> <p>a. Please provide a copy of the policies and procedures used in collecting, safeguarding, storing, and destroying customer information.</p> <p>b. Please provide company policies and procedures for processing customer payments (both electronic and paper transactions).</p>	<p>a. Provided as part of DR-1, Item 2.</p> <p>b. Electronic (credit/debit, ATM, ACH credit, ACH debit, etc) and walk-in payments at contact agent stations are automatically posted to customer accounts as soon as they are received. AT&T's internal objective is to process 99.8% of all payments the day they are received. The internal objective to research and correct all unapplied payments in less than 5 days from receipt of the claim. AT&T asserts they have an extensive data security program that meets or exceeds all industry standards for protection of sensitive data. Customer financial information is only available to those employees with a direct need to know and then only through controlled systems or processes. All sensitive customer information stored on recurring electronic payments is encrypted. Methods, policies, and procedures governing the handling of sensitive customer information are formally documented. Employee training and review processes are in place to ensure that employees know what is / is not permissible with regard to safeguarding sensitive customer data. See <i>Credit and</i></p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p> <p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
	<p><i>Collections Pinless Debit</i> (on disk provided by AT&T), <i>Credit Card Payment ABPS/Terminals</i>, provided as a paper attachment,</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	
<p>18. Please describe how the company conducts initial and recurrent training for employees relevant to data security policies, practices, and procedures.</p> <p>Please provide a copy of current training materials relevant to security of sensitive customer information.</p>	<p>The class "<i>Protecting Information at AT&T</i>" is required for all management employees. For 2008 this class is included in the formal AT&T Corporate Compliance program. As part of this program, employees affirm intent to comply with <i>Information Security Policy and Requirements</i> using a written acknowledgment form (pg 37). See <i>Protecting Information at AT&T</i>, dtd 08/07.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>All have initial training and recurrent training.</p> <p>[REDACTED]</p>

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
			<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div>	
<p>19. Does the company allow authorized third parties to access its internal system infrastructure? If so, how is access to sensitive company and customer information protected from access by unauthorized third party employees?</p>	<p>Access to internal AT&T systems is allowed but determined and authorized by the Business Unit responsible for managing the services provided by the third party. All employees of the third party must sign a non-disclosure agreement or be covered under a non-disclosure signed by the third party company representative that clearly states how sensitive AT&T company and customer information is to be protected. Third party employees must agree to comply with all applicable AT&T data security policies and procedures including computer asset protection requirements as defined by the Chief Security Office (CSO) Security Policy and Requirements (ASPR) documentation. Such policies and procedures ensure governmental and other regulatory requirements are met re protection of customer information and the prevention of unauthorized disclosure.</p>	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div>	<div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: black; width: 100%; height: 15px; margin-bottom: 5px;"></div>	<p>NONE</p> <p>All companies allow third party access.</p> <p>All require thrid parties to follow the same rules as company employees.</p>
<p>20.</p>	<p>2,319</p>	<div style="background-color: black; width: 100%; height: 15px;"></div>	<div style="background-color: black; width: 100%; height: 15px;"></div>	

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>Please provide the number of associates in subsidiaries and affiliated companies, or third party vendors, who have access to customers' full social security account number, banking information, address, date of birth, and/or driver's license number.</p>		[REDACTED]	[REDACTED]	
<p>21. Please describe controls in place to prevent disclosure of customer's personal information by third party vendors.</p> <p>a. What information security training do third party employees receive?</p> <p>b. Does your company conduct background checks or require that background checks be conducted on third party employees?</p> <p>c. Are third party employees with access to company sensitive customer information required to read and acknowledge the same privacy policies or Code of Ethics as company employees?</p>	<p>a. All third party employees are educated on AT&T security requirements as part of the process described in Q 19 (responsible Business Unit determines required access levels and authorizes it. All employees must sign a non-disclosure agreement or be covered by one signed by the third party representative). Training is available on the general aspects of AT&T security requirements and additional training requests may be made by AT&T at its discretion.</p> <p>b. Yes</p> <p>c. Yes</p>	[REDACTED]	[REDACTED]	[REDACTED]
<p>22.</p> <p>a. Please provide a list of any internal audits, external audits, or external studies conducted by, or for, the company during the last 24 months regarding data security.</p> <p>b. Please include the report date, title, a description of the scope and any findings, and the name(s) of the auditor(s).</p>	<p>9/27/07 UNIX Security Review; 12/7/07 Customer Payment Information Security; Customer CPNI, 12/06; Firewall Configuration 02/07; eCredit Card Follow-Up, 05/06</p>	[REDACTED]	[REDACTED]	[REDACTED]

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
<p>c. Please provide a copy of any management responses to these audits.</p>		<p>[REDACTED]</p>		
<p>23. Please provide an incident description and explanation of remedial actions for security breaches from January 2006 through January 2008 for:</p> <p>a. Any sensitive customer information, including but not limited to credit card, bank account, driver's license, and social security account numbers.</p> <p>b. Theft, loss, or compromise of company laptop computers or other portable storage devices such as storage disks, hard drives, pin drives, and personal data devices.</p>	<p>a. No instances of theft, loss or compromise to company portable storage devices were reported during this period other than the laptops mentioned below.</p> <p>b. 2006 - Five computer thefts occurred in BellSouth Florida. None contained sensitive customer info. Seven investigations into allegations of unauthorized access to customer account information/records were conducted for wireline customers. Six were unsubstantiated, <u>one was substantiated</u>. None involved customer credit card or driver's license information. Consistent with the Code of Business Conduct, appropriate disciplinary action was taken.</p> <p>2007 - Eleven computers were stolen; two were recovered. None contained sensitive customer information. Six investigations into allegations of unauthorized access to customer account information/records were conducted for wireline customers. Five were found to be unsubstantiated, <u>one was an instance of an unauthorized family member accessing customer account information</u>. Consistent with the Code of Business Conduct, appropriate disciplinary action was taken.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>POSSIBLE: (AT&T) Not a finding (yet); Discern whether any thefts involved compromise to social security numbers.</p>

Review of Customer Data Security of Florida ILECs ILEC Comparative Chart

Question	AT&T	Embarq	Verizon	Possible Finding
			<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
<p>24. How does the company internally assess the organization's information and customer data security practices?</p> <p>Please describe policies and procedures which govern such assessment, including the frequency, scope, and recommendation implementation.</p>	<p>Two processes for assessing compliance with AT&T Security Policy Requirements (ASPR); internal audits and the Security Evaluation Program (SEP). Internal audits conducted by AT&T Audit Services. SEP is conducted by the CSO organization. Focused on vulnerability, discovery, tracking of compliance with ASPR requirements and reporting via scorecards. Potential weaknesses are ID'd. Each business unit works with SEP to develop resolution and risk mitigation strategies. Scorecards track results; distributed to business unit monthly and VP's quarterly.</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>	
<p>25. Are any internal or external audits planned in 2008 relevant to the security policies, practices, or procedures associated with protection of sensitive customer information? If so, please provide:</p> <p>a. Intent,</p> <p>b. Scope,</p> <p>c. Timeline, and</p> <p>d. Auditor(s)</p>	<p>AT&T is currently in the planning stages of an audit (Privacy of Customer Information). No specifics at this time. Planning to be completed by 5/31/08. The assigned auditor is Ms. Glenda Jones.</p>	<p>[REDACTED]</p> <p>[REDACTED]</p>	<p>[REDACTED]</p>	<p>POSSIBLE (AT&T) Not a finding; follow-up required to determine schedule, scope, and timeline.</p>

Review of Customer Data Security of Florida ILECs

ILEC Comparative Chart

Question	AT&T	Embargo	Verizon	Possible Finding
		[REDACTED]		