

Gramm-Leach Bliley Act Compliance Report

Designated Official: _____

Time Period: 09:53:07 Thursday, July 07, 2005

What is GLBA?

The "Gramm-Leach Bliley Act" (GLBA), also known as the Financial Services Modernization Act of 1999, mandates that financial institutions protect the security and confidentiality of their customers' personally identifiable financial information.

To whom does GLBA apply?

This law applies to financial institutions such as banks, security firms, insurance companies, etc. that sell financial products and services to consumers. They are required to ensure the security and confidentiality of consumer financial information against "reasonably foreseeable" internal or external threats.

How does GLBA affect IT?

From an IT security perspective, financial institutions must implement a process to assess and monitor on a continuous basis the threat environment as well as tools and policies to counter threats. Specific technical safeguards include access control, authentication, encryption, audit controls, and data integrity controls.

To implement the Act, the FTC proposed and passed the Standards for Safeguarding Customer Information (16 CFR Part 314) that are intended to (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Section 314.4 sets forth the general elements that financial institutions should follow as part of their information security program. These elements are as follows:

- a. Requires each financial institution to designate an employee or employees to coordinate its information security program
- b. Requires each financial institution to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- c. Requires each financial institution to design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguard' key controls, systems, and procedures.
- d. Requires each financial institution to oversee service providers by selecting and retaining service providers capable of maintaining appropriate safeguards for customer information.
- e. Requires each financial institution to evaluate and adjust its information security program in light of any material changes to its business that may affect its safeguards.

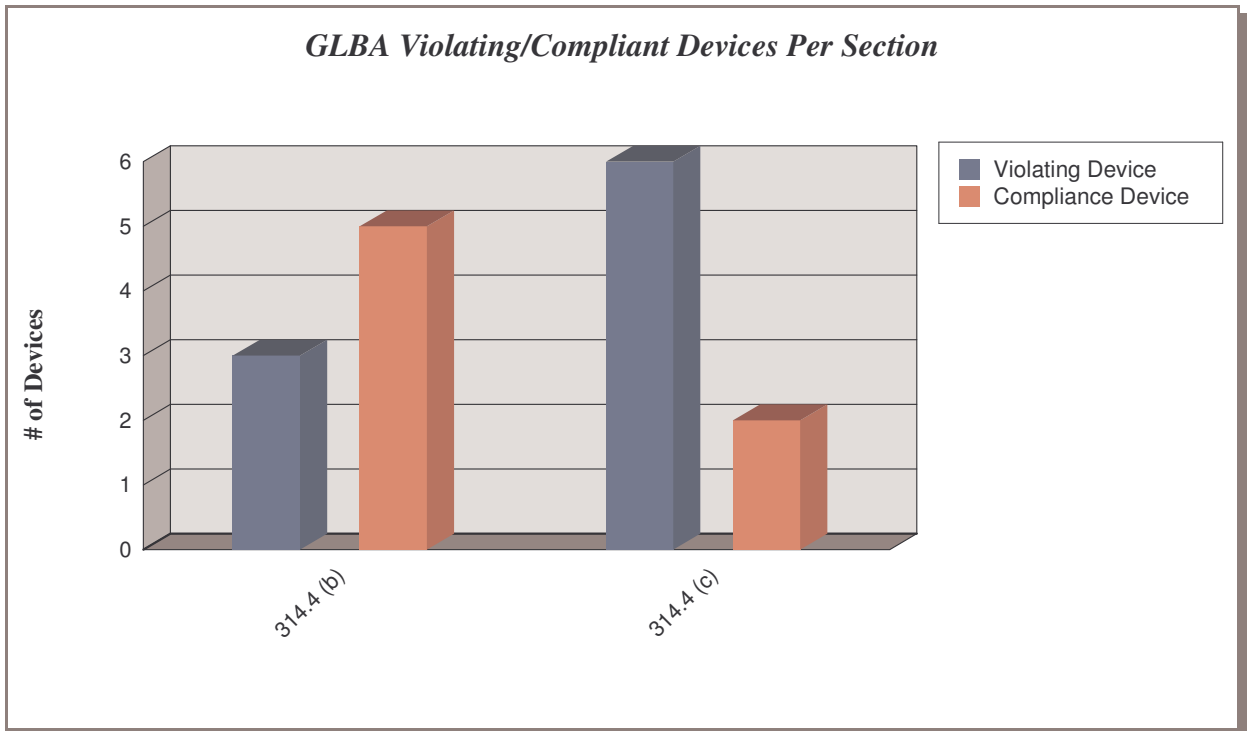
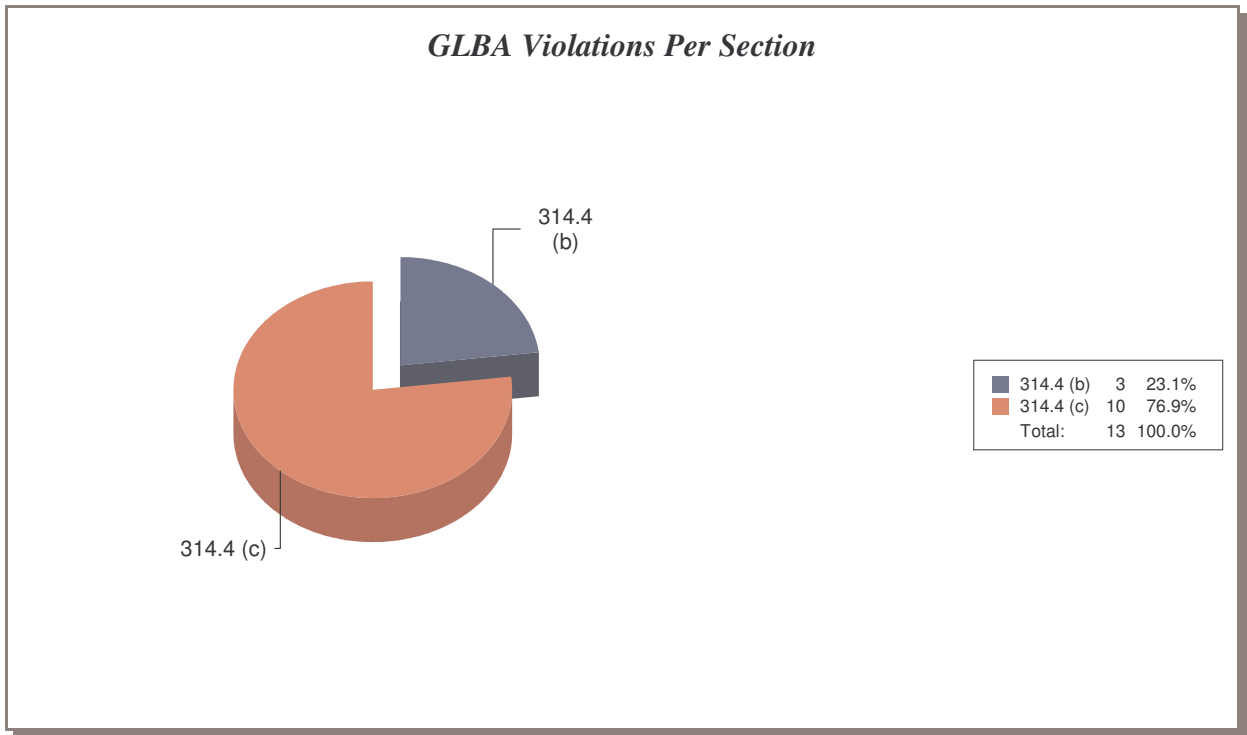
The AirMagnet GLBA Compliance Report

AirMagnet offers regulated entities the ability to comply with the stringent IT security mandates of GLBA. This report covers the major areas of IT security compliance within the context of the GLBA, allowing companies to prove that network security policies are being correctly followed and providing an integral framework to guide network administrators to respond to security threats and incidents in a consistent, compliant, and approved manner.



1/ Policy-Level Compliance Report

This report summarizes your network's compliance on Section 314.4 (b) and (c), showing you the total number of devices that are in compliance or violation of these two provisions.



GLBA IT Security Requirements	Policy Violation	# Violating Devices	# Compliance Devices	Compliance %
314.4 (b)	3	3	5	62.50%
314.4 (c)	10	6	2	25.00%

GLBA Security Requirements			
AirMagnet Alarms	# Violating Devices	# Compliance Devices	Compliance %
Section 314.4 (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of customer information...			
Rogue AP by MAC address (ACL)	3	5	62.50%
Section 314.4 (c) Design and implement information safeguards to control the identified risks.			
Device unprotected by TKIP	1	7	87.50%
AP broadcasting SSID	5	3	37.50%
AP with encryption disabled	3	5	62.50%
WEP IV key reused	1	7	87.50%

Notes:

- 1) By default, your network fails to comply with section 314.4 of the Gramm-Leach Bliley Act if one of the devices violates a security requirements.
- 2) Channel specific policy violations will not be included in the Device-Specific Compliance Report.

2/ Device-Specific Compliance Report

This report contains detailed information about devices in compliance or violation of the DoD Directive. It checks the devices against each and every provision in the Directive to show what policy provisions are violated or upheld to. It lists all wireless devices deployed on your WLAN. The devices can be sort by MAC address, media type, SSID, or vendor.

Device Information	Policy Provisions		Compliance %
	314.4 (b)	314.4 (c)	
MAC Address-Media Channel SSID Vendor			
00:02:6F:20:B3:F7-a Channel: 56 5354a	F	F	0.00%
00:02:6F:04:88:6A-b Channel: 1 1d2d70	P	F	50.00%
00:0F:66:42:D2:B5-b Channel: 11 kassandra	P	F	50.00%
00:02:6F:09:3E:2B-b Channel: 1 1d2d70	P	F	50.00%
00:02:6F:20:B3:F8-b Channel: 11 5354g	F	F	0.00%
00:02:6F:34:A1:59-b Channel: 6 3054g	F	F	0.00%