Rocket

COMPLIANCE

Gramm-Leach-Bliley Act (GLBA) Compliance with Rocket® BlueZone

The Gramm-Leach-Bliley Act (GLBA) establishes a number of control requirements to protect the security and privacy of individuals' financial information. The privacy requirements include disclosures of information that is collected, stored, or distributed and the ability for a customer to opt-out of certain information usages. The security requirements apply to any location, physical or electronic, with a customer's financial data and require both proactive protection measures and breach response procedures.

Specific control implementation requirements related to GLBA are described in "Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards."

Rocket BlueZone terminal emulation solutions provide key control capabilities for protecting your customers' non-public personal information (NPPI). BlueZone does not store any data directly and leverages your host system environment for access controls to protect the confidentiality of NPPI. Enhanced logging and remote access security build upon these logical security controls, and strong encryption capabilities protect all data throughout its usage. Relevant GLBA standards and the capabilities BlueZone offers are listed below.

GLBA REQUIREMENTS	BLUEZONE CAPABILITIES
III(C)(1)(a) Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.	BlueZone provides communication between clients and backend host systems by utilizing the user access permissions inherent to the backend host system environment. BlueZone cannot provide any capability for data access that is not already specifically authorized within your host system O/S to the logged in user. Security Server provides an additional, optional layer of security by acting as a proxy between your host system and clients. Clients must first connect and authenticate to your Security Server using an established user ID, which may be integrated with other Identity Access Management systems including RSA and Active Directory. After authenticating to Security Server, users must then also login to the host system directly, applying the host system-level access permissions. Authentication is performed against the host system directly, applying its password requirements and other authentication mechanisms, which may include physical tokens, client-side X.509 certificates, and other multi-factor authentication systems.
III(C)(1)(c) Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.	BlueZone products supports state-of-the-art encryption methods for all communications between clients and the backend host system environment, including the TLS1.2 are SSHv2 protocols with FIPS-compliant encryption algorithms. BlueZone Web applies this level of encryption to both the end user-to-web server session, and the web server-to-host system session. While support for older protocols is available to support legacy systems, this support can be disabled entirely to prevent any potential security vulnerabilities. In environments where the host system cannot support encrypted sessions, the optional Security Server allows for plaintext communications to be isolated within a secure, local network, while applying strong encryption methods to all external connections with clients.

GLBA REQUIREMENTS	BLUEZONE CAPABILITIES
III(C)(1)(f) An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.	The built-in logging mechanisms inherent to your host system environment record all activities initiated through BlueZone sessions. There is no need to maintain a separate log management function specifically for BlueZone. You can design alerting and monitoring controls around these logs to identify unauthorized access attempts to NPPI. As a supplemental logging mechanism, Rocket BlueZone Web records a log of all client connections to the web server. This does not record commands issued through the sessions, which would be logged through the built-in host system functionality, but provides an additional layer of security by showing how many users and terminals are connecting, when, and from where.
Supplement A, II(A)(1)(a) At a minimum, an institution's response program should contain procedures for assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused.	In the event of a breach, any BlueZone activity from the affected time period would be evidenced in your host system logs for a forensic investigation. BlueZone Web logs can help to identify all terminals and users who have connected to your systems, along with the date, time, and source address.

Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com