Rocket

COMPLIANCE

Gramm-Leach-Bliley Act (GLBA) Compliance with Rocket MultiValue

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 collected, stored, or distributed information, and customers' ability to opt out of certain information usages. The security requirements apply to any physical or electronic location 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."

The Rocket® MultiValue Application Platform (Rocket MV), which includes Rocket UniData and Rocket UniVerse, provides key control capabilities for protecting your customers' non-public personal information (NPPI). Rocket MV enables you to implement strong access rights management and encryption to prevent unauthorized access to NPPI. It includes robust logging and reporting capabilities to assist with your response procedures in the event of a breach. Relevant GLBA standards and the capabilities Rocket MV offers are listed below.

GLBA Requirements	Rocket MV 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.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users. User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users. Audit logs can provide a secure record of any access or updates to user access rights, whether authorized or unauthorized.
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.	OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission. Rocket MV supports robust password and encryption key management solutions for Automatic Data Encryption. Policies can be defined for individual keys. Rocket MV supports the latest implementations of the Secure Shell (SSH) and Transport Layer Security (TLS) encrypted protocols for maximum security.
III(C)(1)(f) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	Audit logs can provide a secure record of any attempted access or updates to customer information in the database, whether authorized or unauthorized. Audit logging configuration is stored in an encrypted file that can be password-protected and is only modifiable by authorized users.

GLBA Requirements	Rocket MV Capabilities
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.	Detailed audit logging and reporting capabilities can assist in your incident response plans by letting you determine exactly which records were accessed, when, and by whom. This will aid in a forensic investigation into the extent of a data breach and the number of affected records.

Rocket

rocketsoftware.com

info@rocketsoftware.com

US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405

twitter.com/rocket

www.linkedin.com/comp
rocket-software

www.facebook.com
RocketSoftwareInc

blog.rocketsoftware.com