IPLocks Information Risk Management Meets the Challenge of Graham-Leach-Bliley Act (GLBA)

January 2005

IPLocks, Inc.

441-A W. Trimble Road, San Jose, CA 95131 USA

www.iplocks.com

IPLocks Information Risk Management Meets the Challenge of Graham-Leach-Bliley Act (GLBA)

By Glinda Cummings, Director, Product Management

The Financial Modernization Act of 1999, also known as the Gramm-Leach Bliley Act provides limited privacy protections against the sale of your private financial information. Sections 6801 through 6809 of the Graham-Leach-Bliley Act (or G-L-B Act as it is otherwise officially designated), impose continuing requirement on financial institutions and other persons and institutions "*…to respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information.*" Avoiding specific guidance or standards on implementation, the Act requires agencies and authorities to "*…establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards….*" Safeguards for customer records and information include:

- Insure *security* and *confidentiality*.
- Protect against anticipated threats or hazards to *security* or *integrity*.
- Protect against *unauthorized access to or use* which could result in substantial harm or inconvenience to the customer.

The intent of the Act is to protect consumer privacy by minimizing the proliferation of non-public personal information by a financial institution directly or indirectly through its affiliates or non-affiliated third-party service organizations. The Act provides rules and guidance on issues of disclosure and information sharing, and providing consumers with opt-out capability.

The Act does not specify any standards of practice or performance to protect the security, confidentiality and integrity of non-public personal information, or to protect against unauthorized access or use. Such standards are left to the "agencies and authorities" that have jurisdiction over the category of financial institutions. Accordingly, the Federal Reserve Board issued Appendix D–2 to Part 208 of Title 12 —Interagency Guidelines Establishing Standards For Safeguarding Customer Information. These guidelines include the following key elements of design for an information security program:

- Establish an Information Security Policy approved by the Board of Directors.
- Assess Risk and Controls:
    - Identify reasonably foreseeable threats and assess the likelihood and potential damage that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
    - Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
- Manage and Control Risk:
    - Design an information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities.
        - Authentication and access controls on customer information systems.
        - Encryption of electronic customer information.
        - Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.

        - Response programs that specify actions to be taken when the bank suspects or detects an attack or intrusion.
    - Train staff to implement the information security program.
    - Regularly test key controls.
    - Adjust the program - Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements.

To ease the pain of GLBA compliance IPLocks Information Risk Management Platform:

- Assesses and monitors database integrity,
- Enhances security and availability,
- Identifies and alerts on potential problems in internal control processes,
- Generates reports and archiving historical activities,
- Provides information for change control compliance, and
- Enables internal auditors and independent audit firms to intelligently assess and monitor internal controls on a recurrent basis.

IPLocks Information Risk Management Platform is a non-intrusive, heterogeneous, external auditing system that helps you mitigate information risk. It does this by assessing vulnerabilities and alerting your personnel to potential problems, monitoring and alerting on unusual database access behaviors, and identifying changes that may violate corporate policy. IPLocks Information Risk Management Platform facilitates G-L-B Act compliance through

- Timely identification of vulnerabilities due to inappropriate database configuration
- Continuous monitoring of changes to database access privileges and roles,
- Alerts on schema changes
- Detection of corrupt or anomalous data and suspicious usage patterns.

IPLocks Information Risk Management Platform assists with timely and effective compliance with the G-L-B Act.

IPLocks Information Risk Management Platform

IPLocks Information Risk Management Platform provides an effective and efficient method of assessing the vulnerabilities of a company's database settings, privilege settings, schema vulnerabilities and data integrity and enables auditors to conduct on-the-spot assessments. IPLocks monitors databases (the source of customer information) through over 100+ pre-defined and user defined rules. It retains audit trails that identify issues and supports investigative steps to facilitate the prevention of insider tampering. The audit trail evidence results in an accurate and unbiased assessment and identification of potential risks and compliance failures. IPLocks Information Risk Management Platform:

- Continuously monitors with minimal human interaction: "Lobster trap" – capture now and retrieve later.
- Identifies abnormal transactions that fall outside of "best practice" security rules or expected behavior.
- Monitors database privilege and access changes for users, user roles and database objects.
- Creates guard bands on business and audit rules to detect and flag suspicious or abnormal transactions.
- Supports pre-configured integrity checking rules and provides diagnostic alert information for timely evaluation and correction.

- Improves executive confidence in their certification of the effectiveness of internal controls for the reporting period.

With respect to specific G-L-B Act Interagency information security guidelines, the following sections describe the related benefit of IPLocks Information Risk Management Platform:

Information Security Policy

IPLocks Information Risk Management Platform

- Provides insight into the access patterns and use of your data to support policy development, identifying both appropriate and inappropriate access.
- Enables real-time definition of user specific policy-based rules to support monitoring of compliance with approved policies.
- Facilitates development of information security policies that are relevant to your business model and practices.

Assess Risk and Controls

IPLocks Information Risk Management Platform

- Provides an effective method of assessing database vulnerabilities related to database settings, privilege settings, schema vulnerabilities and data integrity.
- Periodically and continuously monitors the structural integrity of internal control infrastructure
- Identifies changes in access behavior that may signal a change in business processes or breakdowns in internal control

Monitor and Test Systems and Controls

IPLocks Information Risk Management Platform

- Monitors the structural database integrity of customer information systems and information through statistical algorithms, and automatically alerts on data anomalies that fall outside of expected behavior.
- Monitors the internal control infrastructure through access behavior patterning, and alerts in near real-time of changes in behavior that may reflect internal control changes
- Provides diagnostic information for potential errors and irregularities for evaluation and correction.
- Records and independently archives alerts and associated events to support timely investigation without the risk of insider tampering, providing a more accurate and unbiased event assessment.

Adjust the Information Security Program

IPLocks Information Risk Management Platform

- Generates reports on the assessment of database internal controls
- Archives information about changes in database internal controls
- Provides a layer of database monitoring control to augment the business process internal control system and guard against potential internal control failures
- Provides empirical data to support analysis and decisions on the effectiveness of the information security program.

IPLocks Information Risk Management Platform continuously audits and monitors data integrity, user privileges and role changes, schema structure changes, and usage patterns through pre-defined and user-defined rules to ensure the security, integrity and availability of customer

information and information systems for compliance with the G-L-B Act. Effectiveness is achieved by focusing control directly on the data and monitoring how the information is accessed and used. IPLocks Information Risk Management Platform effectively monitors data, schema and privileges and generates alerts to the appropriate personnel of anomalies and breaches, which may indicate a compromise to the data security and integrity. IPLocks Information Risk Management Platform brings companies one step closer to addressing and conforming to the requirements imposed by the G-L-B Act.

About IPLocks

IPLocks, Inc. protects business continuity, safeguards company brand reputation and eases the pain of corporate governance by securing critical information assets from negligent and malicious acts.

The IPLocks Information Risk Management Platform alerts management to information risks from security and business policy violations, attacks on data, compromised structural integrity and information theft, which other security solutions fail to detect.

IPLocks secures business critical data for financial services, telecommunications, media services, healthcare, public utilities and other industries. Founded in 2002, San Jose, California-based IPLocks is a privately held global corporation with customers throughout North America, Asia Pacific, South America and Europe. For additional information, visit www.iplocks.com.