

Securing Non-Public Personal Information for Financial Service Institutions

How Shalom Security Platform Enforces Gramm Leach Bliley (GLB) Act Compliance

Industry Focus: Any financial institution that offers financial products and services to individuals: banks, mortgage brokers, tax preparers, universities, insurance, investment firms, etc.



In 1999 congress passed the Gramm-Leach-Biley Act to address disclosure of nonpublic personal information. Every financial institution including banks, securities firms, utility companies, etc are required by Law to protect personal data of their customers. The law defines the term "financial institution" to mean any institution: the business of which is engaging in financial activities as described in section 1843(k) of title 12 USC, which includes, banks, investment companies, insurance companies, public utilities, universities, and others.

In effect, companies and institutions that handle public records are not only obligated to ensure that they have sufficient information security controls, but also adequate controls to stop the "misuse" of non-public personal information by malicious company insiders. With respect to insider information security, the GLBA requires all institutions that handle nonpublic information to create implement and enforce insider security policies and controls that will:

1. Ensure the security and confidentiality of customer records (from intruders).
2. Protect against any anticipated threats or hazards (including insider threats) to the security of such records.

3. Protect against the unauthorized access or use of such records/information in ways that could result in substantial harm or inconvenience to customers.

SHALOM SECURITY PLATFORM PROTECTS NONPUBLIC PERSONAL INFORMATION BY CATCHING MALICIOUS INSIDERS AND LOCKING OUT INTRUDERS INSIDE THE NETWORK

While computer security systems like passwords, smart cards, and firewalls protect data from outsiders, they do not address internal security threats. Many computer security breaches occur within an organization and are executed by malicious insiders. People lie at the heart of insider security breaches and most of these incidents never get detected.

Nowell Shalom Security Platform protects customer data by constantly looking out for suspicious user activity from either malicious insiders or impostors within the network.

- For intruders who penetrate computer systems using stolen passwords, Shalom Security Platform ejects them and keeps them locked out site-wide when they fail the identity verification. It also reports “phony” backdoor accounts and implanted automated scripts.
- In real time, Shalom Security Platform questions and reports malicious insiders the very minute they behave suspiciously, disrupting and deterring them from stealing customer financial records.

The Safeguards Rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions such as credit reporting agencies that receive customer information from other financial institutions.