



A Websense® Research Brief

GLBA Compliance Requires that Leaks be Sealed

Modernizing Financial Privacy

Financial institutions must protect customer privacy and adhere to regulatory requirements. The Gramm-Leach-Bliley Act of 1999 (GLBA) restricts the sharing of private customer data; even the accidental loss of sensitive information can trigger profound consequences. Not just limited to banks, GLBA applies broadly to the financial community. It affects financial institutions such as non-bank mortgage lenders, insurance companies and investment advisors. In addition to formulating a privacy policy, financial institutions must implement “administrative, technical and physical safeguards”, according to the Federal Trade Commission.

Information control is at the heart of GLBA. Specifically, financial institutions must:

- Ensure the security and confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Stop unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer

GLBA compliance requires both internal and external safeguards. Though the external threat receives the most attention, the improper use of customer information internally is actually an even greater problem. Information leaks are most often caused by employee error or negligence and can result in considerable customer inconvenience or harm, despite the fact that often no malice was intended. Leak prevention is a crucial component in information control and thus should be included in any GLBA compliance initiative. Information leaks can be as damaging as they are common, yet they are easily preventable. Threats from the outside require responsiveness; internal leaks can be reduced simply through rigorous planning and improved operations.

While GLBA compliance is mandatory, its provisions make sense. The measures included in GLBA can reduce the substantial risk associated with leaking sensitive customer data. According to Forrester, a single leak event can cost a company \$128 per record (including impact and opportunity costs); letting 10,000 records slip could lead to a total cost of \$1.28 million. Leak prevention leads to the mitigation of business and IT risk as well as compliance with GLBA.

Preventing Privacy Breaches

According to the Ponemon Institute, less than 15% of information loss comes from internal theft and malicious employees (combined). But, more than 80% of leaks results are unintentional or mistakes. An employee copies data to a drive that is exposed to the Web or sends a customer record to the wrong email address. Fortunately, these mistakes are the easiest to control. Unlike the outside environment, you have the ability to reshape operations to reduce risk and improve employee behavior.

GLBA compliance requires a rigorous control framework governing internal and external communications. In addition to preventing your staff from leaking sensitive information (e.g., personally identifiable information (PII), account balances, or communications with a financial advisor) to the outside world, organizations need to build internal controls. This could include limiting the internal use of customer data for marketing purposes or other business analysis. The obligation under GLBA is to maintain the integrity of customer records and ensure that the use of such data does not lead to customer harm or inconvenience.

Information leak prevention (ILP) technology focuses specifically on keeping sensitive data inside the company. ILP facilitates GLBA compliance by monitoring all communication protocols in the enterprise to identify potentially private data and prevent it from reaching the outside world. ILP solutions look for data that is likely to be sensitive in order to intercept it before it leaves the safety of your company's infrastructure. Traditionally, regular expression analysis has been ILP technology's core. The solution examines the data itself in order to discern between leak and business as usual.

Regular expression analysis has its limits, though. Without any indication of data's context, ILP solutions tend to yield high rates of false positives (not actually leaks) and false negatives (missed leaks). As a result, prevention can result in considerable excess work for little protection. In order to provide sufficient information control, ILP solutions need more than regular expression analysis. Some consideration of context is necessary to distinguish between sensitive and innocuous data.

Controlling Content through Context

The Websense® Content Protection Suite uses both content and context awareness to provide Deep Content Control (DCC). DCC applies contextual indicators including data source, related data elements (e.g., in a database table), the number of records being sent, destination, and user information in order to decide whether a communication is a potential leak or simply the normal course of business. This level of granularity and control helps improve leak prevention, achieve GLBA compliance, and mitigate risk. Context-awareness data evaluation reduces the number of false negatives and false positives. In addition to yielding more accurate results, DCC reduces the leak-related workload of business unit leaders and other staff members.

Content Protection Suite accelerates GLBA compliance by offering pre-configured information leak rules designed specifically for this purpose. You can use out-of-the-box GLBA functionality to get started and modify the rules over time as internal policy evolves. Instead of having to start with an extensive requirement and design endeavor before deriving any value from a leak prevention solution, Content Protection Suite delivers an immediate return on investment through pre-configured logic, and tailoring the logic to your specific GLBA compliance policies can be accomplished over time and without disrupting the near-term benefits of the solution's out-of-the-box logic.

After implementing Content Protection Suite, for example, you may decide that it is necessary—as a result of company policy, operations, or observed results—to modify the sensitivity of the logic. If the rules are too strict, generating a high volume of suspected

leaks, you can alter the rules slightly to affect the system's behavior. One way is to require that multiple records be communicated in order to trigger a leak. An email with one record is likely to be business as usual; five customer records in one email message, though, may be abnormal. With Content Protection Suite, you can use the number of records communicated to massage the sensitivity of your information controls without substantially changing the core logic. For specific situations, you can create rules from scratch to implement and enforce specific policies.

GLBA compliance may be standard, as dictated by the law, but your business is not. Regulatory compliance must account for your unique business environment to protect your company and customers. Content Protection Suite uses Deep Content Control to prevent leaks and pre-defined GLBA logic to get you started. As your governance framework matures, your ILP efforts can grow through modifications to existing rules and new controls, providing the flexibility required to integrate with your business processes without sacrificing compliance.