



Safeguarding Financial Privacy

The purpose of this whitepaper is to illustrate how enterprise single sign-on can help financial institutions oversee service providers in compliance with the GLBA while ensuring only authenticated employees access financial data.



WHITE PAPER

Single Sign-On – One Step in Assuring Service Providers Protect Your Customers' Personal Financial Data

Introduction

Protecting consumers' personal financial information held by financial institutions is the primary objective of the Gramm-Leach-Bliley Act or GLBA, a.k.a. The Financial Modernization Act of 1999. Financial institutions collect personal information, names, addresses and phone numbers; social security numbers, bank and credit card account numbers; and income and credit histories in their daily business transactions with customers. Records of any form – electronic, paper or other media – containing non-public customer information must be kept private and the requirement extends to any method by which the information is obtained. The GLBA covers financial institutions regardless of whether they have one hundred customers or one million, offer online or traditional services, and outsource or maintain their own systems and operations. Financial institutions must take steps to secure customer data from unauthorized access in order to comply with this federal law. Their governing bodies, which can range from the Federal Deposit Insurance Corporation (FDIC) to the Federal Trade Commission (FTC), have to periodically audit and enforce compliance through examinations that can result in fines for non-compliance.

Three Parts to Secure Privacy

The privacy requirements are comprised of three principal parts: the Financial Privacy Rule, Safeguards Rule and Pretexting provisions. The Financial Privacy Rule seeks to protect non-public personally identifiable financial information from unauthorized parties. Non-public information is data collected about a consumer in conjunction with providing a financial product or service, such as outstanding loan balances.

To protect non-public customer information, financial institutions are required by the Safeguards Rule to design, implement and maintain standards. 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. In other words, service providers or third-party vendors are also mandated to protect non-public customer information.

“Pretexting” - the practice of obtaining customer information from financial institutions under false pretenses - is prohibited under the Pretexting provision. The Federal Trade Commission or FTC has brought several cases against information brokers caught pretexting. Identity theft is the fastest growing crime according to the FTC, so customers are increasingly anxious about the actions that financial institutions are taking to secure their personal data.

Governing Authorities

Eight federal agencies and the states are authorized by the GLBA to administer and enforce the Financial Privacy Rule and the Safeguards Rule. For example, the FTC can enforce the law with respect to “financial institutions” that are not covered by the federal banking agencies, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and state insurance authorities. Among the institutions under FTC jurisdiction for purposes of the GLBA are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors

This paper consists of an overview of the Gramm-Leach-Bliley Act with a unique focus on the Safeguards Rule and its impact on the agreements financial institutions undertake with service providers and other institutions. Financial institutions often outsource key operations, such as teller operations and equipment leasing services. One way to ensure service providers protect access to non-public personal financial information is to require implementation of enterprise single sign-on. Enterprise single sign-on is a simple, yet highly effective way to (1) tie together proper user authentication and application access and (2) enable proper privacy controls. One ID and password authenticates the user for all required applications, such as identity verification and creditworthiness assessment. Single sign-on makes it possible to require strong passwords (complex and frequently changed) on all applications that access non-public data.

Single sign-on eliminates the need for financial professionals to remember multiple passwords, while retaining a high level of security for each application. A financial professional can access customer records, account balance information, and other financial data using one time authentication. Of greater significance to any financial institution doing business with third-party vendors is the ability to guard information not under its direct control from improper usage and distribution. Authentication as part of a written, comprehensive security program is critical since it allows for a way to log who is attempting to access specific information and when. This audit trail of every record accessed can be supplied to governing authorities during an examination of a financial institution's security standards as required by GLBA.

Disclosure of non-public personal information is never permitted, except as allowed by law to provide products and services to the customer. Financial privacy starts with enterprise single sign-on – one giant step toward assuring customers and regulatory agencies that access to non-public data is restricted to authenticated personnel.

Overview of the Gramm-Leach-Bliley Act

The GLBA restricts the ability of financial institutions to sell, give, or otherwise disclose personal information to third parties without permission. The law requires that financial institutions protect information collected about individuals - not information collected in business or commercial activities. A financial institution is any organization in the business of engaging in activities that are financial in nature, or incidental to such activities. This includes national banks, federally chartered thrifts, FDIC depositories, insurance companies and agencies, mortgage lenders, securities firms and other firms that offer financial products and services. Consumers must receive privacy notices explaining the institutions' information-sharing practices. In turn, consumers have the right to limit some - but not all - sharing of their information. Distinction between Consumers and Customers

A company's obligations under the GLBA depend on whether the company has consumers or customers who acquire its services. A consumer is an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons. A customer is a consumer with a continuing relationship with a financial institution. Generally, if the relationship between the financial institution and the individual is significant and/or long-term, the individual is a customer of the institution. For example, a person who gets a mortgage from a lender or hires a broker to get a personal loan is considered a customer of the lender or the broker, while a person who uses a check-cashing service is a consumer of that service.

The difference between consumers and customers is important because only customers are entitled to receive a financial institution's privacy notice automatically. Consumers are entitled to receive a privacy notice from a financial institution only if the company shares the consumers' information with companies not affiliated with it, with some exceptions. Customers must receive a notice every year for the duration of the customer relationship. However, privacy extends to all consumers.

The Privacy Notice

The privacy notice must be a clear, conspicuous, and accurate statement of the company's privacy practices; it should include what information the company collects about its consumers and customers, with whom it shares the information, and how it protects or safeguards the information. The notice applies to the "non-public personal information" the company gathers and discloses about its consumers and customers; in practice, that may be most - or all - of the information a company has about them. The privacy notice must be given to individual customers or consumers by mail or in-person delivery. Reasonable ways to deliver a notice may depend on the type of business the institution is in: for example, an online lender may post its notice on its website and require online consumers to acknowledge receipt in order to process a loan application.

Opt-Out Rights

Consumers and customers have the right to opt out of - or say no to - having their information shared with certain third parties. The privacy notice must explain how to opt-out and offer a convenient way to do so. A simple opt-out method is to provide a toll-free telephone number or a detachable form with a pre-printed address.

The privacy notice must explain that consumers have a right to say no to the sharing of specific information - credit report or application information - with the financial institution's affiliates under the Fair Credit Reporting Act. An affiliate is an entity that controls another company, is controlled by the company, or is under common control with the company. An individual cannot opt out if:

- a. a financial institution shares information with outside companies that provide essential services like data processing or servicing accounts;
- b. the disclosure is legally required;
- c. a financial institution shares customer data with outside service providers that market the financial company's products or services.

Receiving Non-public Personal Information

The GLBA puts some limits on how anyone that receives non-public personal information from a financial institution can use or share the information. Let's look at a lender that discloses customer information to a service provider responsible for mailing account statements, where the consumer has no right to opt out: The service provider may use the information for limited purposes - that is, for mailing account statements. The information cannot be sold to other organizations or used for marketing.

When a company receives nonpublic personal information from a financial institution that provided an opt-out notice -- and the consumer didn't opt out, the recipient steps into the shoes of the disclosing financial institution. It may use the information for its own purposes or distribute it to a third party, consistent with the financial institution's privacy notice.

Other Privacy Provisions

Other important provisions of the GLBA also impact how a company conducts business. For example, financial institutions are prohibited from disclosing their customers' account numbers to non-affiliated companies when it comes to telemarketing, direct mail marketing or other marketing through e-mail, even if the individuals have not opted out of sharing the information for marketing purposes.

Service Providers and The Safeguards Rule

The FTC issued the Safeguards Rule to require financial institutions under its jurisdiction to safeguard customer records and information from internal and external threats. The rule applies to individuals or organizations that are significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, non-bank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.

The Safeguards Rule mandates that financial institutions develop a written information security plan that describes policies to protect customer information. All programs must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. Covered financial institutions must:

- a. assign an employee or employees to coordinate safeguards;
- b. identify internal and external risks to the security, confidentiality and integrity of customer information and evaluate the effectiveness of current safeguards;
- c. design a safeguards program, and detail the plans to monitor its efficacy;
- d. select and retain appropriate service providers and require them contractually to implement and maintain the safeguards; and
- e. assess the security program periodically and adjust it to reflect changes in the business climate.

Although each information security program must include these basic elements, the Safeguards Rule is flexible enough to allow each financial institution reasonable discretion to design an information security program that suits its particular size, complexity and type of activities.

Experts suggest that three areas of operation present special challenges and risks to information security: employee training and management; information systems, including network and software design, and information processing, storage, transmission and retrieval; and security management, including the prevention, detection and response to attacks, intrusions or other system failures. Financial institutions are mandated to pay special attention to these areas by defining specific measures to manage the risks posed. Measures can include antivirus software, firewalls, password resets, authentication software and smart cards.

Oversight of Service Providers

Many financial institutions don't realize that they are now required to protect customer information provided to a service provider by overseeing their service provider arrangements. A "service provider" is any person or entity that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the bank. Data processing companies, securities clearinghouses, and check printing operations are in this category.

Oversight measures include exercising appropriate due diligence in selecting service providers; requiring service providers to implement appropriate security measures; and, depending on the financial institution's risk assessment, monitoring service providers to confirm they have established adequate policies in accordance with the Safeguards Rule.

Contract Review

Pursuant to oversight, some of the key points that service provider contracts should address, include:

- a. How does the financial institution assess risk to its customer information systems?
- b. Does the risk assessment include vendor oversight requirements?
- c. What is the service provider's response when it suspects unauthorized access — Are procedures in place to prevent and/or report unauthorized access to the financial institution?
- d. Does the service provider contract provide for sufficient reporting on the part of the service provider to allow the financial institution to appropriately evaluate the service provider's performance and security, both in ongoing operations and when malicious activity is suspected or known?

All service provider contracts should contain language to the effect that the service providers have implemented procedures to safeguard the security and integrity of data disclosed to them. The Safeguards Rule states that provisions for reporting attempted or actual security breaches and evaluating the service provider's data security performance should exist in every service provider contract.

Managing and Controlling Risk

As part of a comprehensive risk management plan, the financial institution should establish written policies and procedures to adequately control the identified risks and achieve the overall information security objectives. Policies and procedures should match the sensitivity of the information as well as the complexity and scope of the institution and its activities. In establishing privacy policies and security procedures, each financial institution should consider suitable:

- a. Access rights to customer information;
- b. Access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies;
- c. Access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities;
- d. Encryption of electronic customer information, including while in transit or in storage on networks or systems;
- e. Procedures to confirm that customer information system modifications are consistent with the information security program;
- f. Dual control procedures, separation of duties, and employee background checks for employees with access to customer information;
- g. Contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by service providers;
- h. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

- i. Response programs that specify actions to be taken when unauthorized access to customer information systems is suspected or detected
- j. Protection against physical destruction of customer information; and
- k. Disaster recovery programs to preserve the integrity and security of customer information in the event of computer or other technological failure.

Staff should be trained to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information. Ongoing training of personnel on the provisions of the GLBA and the privacy notice requirements of the institution is necessary.

Key controls, systems and procedures of the information security program should be regularly tested and reviewed by independent third parties to confirm that they control the risks and achieve the overall objectives of the institution's information security program.

The information security program must be monitored, evaluated and adjusted in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

The financial institution has ultimate responsibility for safeguarding customer information even when it gives a service provider access to that information. Confirming that service providers have implemented an effective information security program to protect customer information is critical. Contractually obligating service providers to use enterprise single sign-on as a safeguard builds a foundation for consumer trust.

Privacy regulations are on the rise. California recently passed a law that requires companies to publicly disclose when they are the subject of network intrusions or "hacks" that result in security breaches of customer and employee information. The law applies to any company doing business in California that stores data about California residents, regardless of the location of the compromised network and data. Analysts estimate that credit-card issuers lose \$1 billion to \$3 billion each year to fraud resulting from the theft of credit card information. California has enabled its residents to lock down their credit reports to prevent misappropriation by hackers. Other states are sure to follow. The federal government is considering removing social security numbers from all public records. Therefore, any financial institution that wants to avoid negative publicity and fines had better know what their service providers are doing to prevent unauthorized access and misuse of their customers' non-public data before entrusting them with key operations.

Why Implement Enterprise Single Sign-On?

Under GLBA, institutions are required to evaluate potential threats and protect against the unauthorized use or disclosure of non-public personal financial data. A check printing operation might differ from a large mutual fund company in its privacy policies. The end goal is always the same – to do everything reasonably possible under the circumstances to protect non-public personal information. In order to control access to customer information, formal policies and procedures can be implemented that allow different levels of access to financial information. No single policy, practice or tool can ensure effective overall security. Most financial institutions have always been concerned with the privacy of their customers' information. The GLBA requires financial institutions to employ extensive physical,

electronic, and procedural controls to protect customers' personally identifiable financial data. This is essential in light of the rapid growth of online services, such as paying bills, transferring funds, and trading stocks. One of the easiest, fastest and most effective technologies to institute and document compliance is enterprise single sign-on. Financial applications are often not properly locked down – many users are under one account. Financial institutions and their service providers need to assure that applications are password protected in order to prevent improper access. Sometimes many users share one password, but GLBA mandates an audit trail. One password would make it difficult to track usage and culpability. Users need individual passwords with strict selection criteria to make it more difficult for the criminal to gain access. Passwords should be changed regularly to keep systems secure.

Single sign-on makes it easy for every user to start every computerized session with proper authentication. The result is simple to use security combined with verified privacy. Audit trails facilitate accountability for personally identifiable information usage. Single sign-on does not mean that all applications use the same password. Users often confuse single sign-on with password synchronization, an older method for distributing and synchronizing a main password to other systems. True single sign-on solutions enable users to have different passwords for every application, store these passwords in a protected database and make them available to the users upon login. The SSO solution will retrieve the password from the database upon receiving a request for access – the login is transparent to the user.

Budget considerations often factor into security decisions. Biometrics, smart cards and public key infrastructure are more expensive and time-intensive security technologies to implement. Enterprise single sign-on does not preclude applying those technologies in the future. However, an effective enterprise single sign-on product can be installed rapidly at a reasonable cost to quickly meet the minimum standards mandated by the GLBA. There is no burden of application integration with an effective enterprise single sign-on solution. Service providers can leverage current infrastructure and keep their financial customers' information secure.

CONCLUSION

Enterprise single sign-on can help financial institutions oversee service providers in compliance with the GLBA as well as ensure only authenticated employees access financial data. Enterprise Single Sign-On automates every password management task for financial professionals with a legitimate need to access personal financial data. SSO helps:

- a. make it possible to implement appropriate authentication and related security policy,
- b. assure a financial institution can confidently provide secure access to personal financial data
- c. lock down applications
- d. track usage of non-public financial data and
- e. simplify compliance for the service provider.

Properly implemented, SSO maintains the security of countless applications, tracks and logs access of financial information and speeds access to critical information. It is an effective method of authorizing access to personal financial data and resources - holding staff accountable for their activities. By deploying an enterprise single sign-on solution, financial institutions and their service providers can substantiate that a reasonable effort to protect consumers' privacy by ensuring secure and reliable access is ongoing Enterprise Single Sign-On – a sound business practice for assuring service providers protect consumers' sensitive information as if it were their very own. When information is shared safely, a customer's identity should remain right where it belongs – in his or her private file. Financial institutions and their service providers can use single sign-on to keep their customers' data in the privacy vault.

passlogix®

V-g@®

WHITE PAPER

75 Broad Street, Suite 815, New York, NY 10004

Tel: 212.825.9100 x 2

Or : 866.727.7564 x 2

Fax:212.825.0326

Web: www.passlogix.com

E-mail: sales@passlogix.com