okta

Your GLBA compliance journey with Okta

Introduction

The Gramm-Leach-Bliley Act (GLBA) is a United States Federal law that mandates that financial institutions disclose their information-sharing practices to their customers and proactively secure sensitive data. Also known as the Financial Modernization Act of 1999, the GLBA was focused on updating and modernizing the financial industry. Today, all companies that offer consumers financial products or services like loans, financial or investment advice, or insurance are required to comply with GLBA, which is broadly divided into two sections:

I. The Safeguards Rule
II. The Financial Privacy Rule

The Safeguards Rule

Put simply: financial institutions must protect the customer information they collect.

Before we dig into the specifics of what that means, let's first make sure we're clear on who must comply. Under the GLBA, 'financial companies' includes a broad range of businesses of all sizes: any organization that is 'significantly engaged' in providing financial products or services. That includes any business that collects personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and social security numbers.

More tangibly, that could include check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguard Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions.

To comply with the Safeguards Rule, companies must develop a written information security plan that describes how they protect customer information. The requirements are flexible depending on the company's size, complexity and circumstances, and are ultimately designed to ensure financial institutions assess and address the risks to customer information in all areas of their operation. The three areas that the GLBA identifies as particularly important in information security are:

1. Employee Management and Training
2. Information Systems
3. Detecting and Managing System Failures

Identity and access management security can play a key role across all three of these categories. Under the Employee Management and Training area, for example, the FTC identifies identity-oriented projects such as "*Preventing terminated employees from accessing customer information by immediately deactivating their passwords and usernames and taking other appropriate measures.*" Or, as a part of Information Systems security, the FTC identifies

> *"Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information."*

The Financial Privacy Rule

Under this rule, financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to opt-out.

As with the Safeguards Rule, all 'financial institutions' as defined above must comply with this Privacy Rule. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information. When GLBA says 'consumer personal information', it refers to nonpublic personal information (NPI), or any personally identifiable financial information that is not otherwise publicly available. For example, name, address, income, SSN, court records or other information from a consumer report, credit or debit card purchases, etc. It does not include information that has been made publicly available, i.e. information that has been widely distributed in the media or government records made available to the public.

Financial institutions must give their customers clear and conspicuous written notice describing their privacy practices and policies. Please note, the Okta service is out of scope with regards to the creation or distribution of privacy practices as well as alerting customers and consumers of their right to opt-out.

How Okta Can Help

In addition to developing their own safeguards, companies covered by the GLBA are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

While Okta is out of scope for GLBA for our financial customers, Okta does conform with its requirements and therefore organizations can leverage GLBA data in their Okta tenant. In the table below, you can find GLBA control mapping for using the Okta service in your organization.

Additional Resources

Okta has made its privacy policy and documentation available online, accessible via the links below. For additional information on Okta's approach to privacy and security, including additional compliance certifications and information, visit:

- Okta Blog: What is GLBA compliance?
- Okta Trust Site: Security
- Okta Trust Site: Compliance
- Okta Privacy Policy
- Okta Security & Privacy Documentation

Appendix A (if customer is leveraging Okta):

		GLBA	
Requirements	**Is Okta compliant**	**Safeguard rule**	**Privacy Rule**
Checking references or doing background checks before hiring employees who will have access to customer information.	Yes	Customer responsibility	Conformance to the Privacy rule in its entirety is the customer(s) responsibility
Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.	Yes	Customer responsibility	
Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.	Yes	Customer responsibility	
Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)	Yes	Yes	
Using password-activated screensavers to lock employee computers after a period of inactivity.	Yes	Customer responsibility	
Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.	Yes	Customer responsibility	
Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information	Yes	Customer responsibility	
Regularly reminding all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.	Yes	Customer responsibility	
Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.	Yes	Customer responsibility	
Imposing disciplinary measures for security policy violations.	Yes	Customer responsibility	
Preventing terminated employees from accessing customer information by immediately deactivating their passwords and usernames and taking other appropriate measures.	Yes	Yes	

		GLBA	
Requirements	**Is Okta compliant**	**Safeguard rule**	**Privacy Rule**
Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example: • Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods. • Store records in a room or cabinet that is locked when unattended. • When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area. • Where possible, avoid storing sensitive customer data on a computer with an Internet connection. • Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area. • Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.	Yes	Yes (partial)	Conformance to the Privacy rule in its entirety is the customer(s) responsibility
Take steps to ensure the secure transmission of customer information. For example: • When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. • If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message. • If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.	Yes **Note**: Okta is considered a service provider and not a merchant.	Yes (partial)	
Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example: • Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group. • Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed. • Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information. • Detecting and Managing System Failures. Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:	Yes	Yes	

		GLBA	
Requirements	**Is Okta compliant**	**Safeguard rule**	**Privacy Rule**
Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.	Yes	Customer responsibility	Conformance to the Privacy rule in its entirety is the customer(s) responsibility
Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to: • Check with software vendors regularly to get and install patches that resolve software vulnerabilities; • Use anti-virus and anti-spyware software that updates automatically; • Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations; • Regularly ensure that ports not used for your business are closed; and • Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.	Yes	Yes (partial) **Note**: Okta work force identity products and customer identity are technical controls and enable customers conform to the control requirements.	
Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to: • Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information; • Use an up-to-date intrusion detection system to alert you of attacks; • Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and • Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.	Yes	Yes (partial) **Note**: Okta has a Audit log feature for its customer Admins.	
Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs: • Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet; • Preserve and review files or programs that may reveal how the breach occurred; and • If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.	Yes	Customer responsibility	
Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example: • notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm; • notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm; • notify the credit bureaus and other businesses that may be affected by the breach.	Yes	Customer responsibility	