ARE YOU GLBA COMPLIANT?

An Examination of GLBA & Certification Requirements

SCA
SECURITY COMPLIANCE ASSOCIATES

Security Compliance Associates
2727 Ulmerton Rd, Suite 310, Clearwater, FL 33762 / 1-877-993-4472 / www.scasecurity.com

ELITE PROVIDER 2016 American Land Title Association

LEGAL COMPLIANCE

When it comes to your business, security is everything. The potential loss of customer data could be devastating and could leave your company open to significant liability issues, especially if your policies and practices are not *legally* compliant. A lack of compliance can also put you in a bad position with lenders. After the Consumer Financial Protection Bureau (CFPB) opened its doors in May 2011, it began putting significant pressure on lenders to ensure their third party vendors were regulatory compliant. The CFPB and other federal agencies announced that they planned, under some circumstances, to hold lenders liable for the violations of their vendors. In turn, the lenders made it clear that they expected their vendors to not only be compliant with state and federal regulations, but to be able to show clear documentation of compliance.

The American Land Title Association (ALTA) chartered its seven pillars of Title Insurance and Settlement Company Best Practices in 2013, designed to guide the industry in the implementation of policies and procedures that will provide lenders with the assurances they need.

ALTA's Best Practice 2.0 created a structure and a road map for agents to follow in establishing a compliance baseline. However, as emerging cyber security threats increase in frequency and complexity on a daily basis, it's clear that taking a deeper dive into Pillar No. 3 compliance is essential to ensure safety, as well as complete legal compliance. Although this issue pertains to all of the best practices, it is particularly significant with Pillar No. 3.

ALTA provides significant guidance on how to meet the best practices standards and how to self-assess compliance and receive certification. In fact there are businesses and some accounting firms, that offer programs that evaluate whether a company's policies and procedures conform to best practices.

However, an important question to ask these companies is, "Does your Best Practice Certification ensure compliance with federal and state law?"

When a firm conducts an assessment of your company's implementation of ALTA's best practices and provides you with a certificate or letter of certification, this does not necessarily certify compliance with federal and state legal requirements. If you are having your business practices evaluated, it is important that you ask not only for ALTA best practices certification, but also for an analysis regarding whether you are specifically in compliance with all applicable statutory laws.

BEST PRACTICE PILLAR NO. 3

ALTA's third pillar pertains to the protection of consumers' personal, private information. ALTA outlines the need for companies to: "Adopt and maintain a written privacy and information security program to protect Non-public Personal Information [NPI] as required by local, state and federal law."

Pillar No. 3 provides twenty-six security-related components to ensure NPI security and emphasizes that state and federal laws require companies to have certain procedures in place to protect NPI. When you contract with a company to perform your third-party certification, you also need to verify that they are assessing your IT security posture to ensure you are meeting Gramm-Leach-Bliley Act (GLBA) requirements.

The primary concern is that a company could have policies in place that conform to Pillar No. 3 recommendations but are not fully compliant.

"If you have been certified under pillar 3, you are not necessarily following federal guidelines," said Matthew Froning, Chief Information Officer at Security Compliance Associates. "Whether you are compliant with federal law is not always clear from a review of your policies and procedures. The analysis needs to go much more in depth. It is highly recommended that you have an independent third party looking at your overall security posture and ensuring your written policies and procedures match your operating environment."

Anyone conducting an evaluation of your company should be able to inform you of which data security laws pertain to your company and whether your company is currently compliant in both its policies and its practices. In addition, the firm should tell you whether your policies and practices need to be updated. If a review reveals that you do have risks, you need to understand them and have reasonable mitigation plans to reduce them.

Security Compliance Associates
2727 Ulmerton Rd, Suite 310, Clearwater, FL 33762 / 1-877-993-4472 / www.scasecurity.com

What you need is a company or a group of companies that can assess both best practices and legal compliance.

GRAMM-LEACH-BLILEY ACT

One of the primary federal laws that financial institutions must be aware of is the Gramm-Leach-Bliley Act (GLBA). Under the act, which was enacted by Congress in 1999, financial institutions are required to provide adequate protection and privacy for consumer information. The Federal Trade Commission (FTC) was charged with the responsibility of enforcing the law through a series of rules and regulations. When implementing the GLBA, the FTC promulgated the Safeguards Rule and Privacy of Consumer Financial Information Rule.

If your company is looking for Pillar No. 3 certification, it also needs to be verifying that it is compliant with the GLBA. If the certifying firm is not looking at GLBA compliance, you need to seek out a firm that will.

The Safeguards Rule requires financial institutions to have a written data security plan in place that is "appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles."

In executing its plan, a company is required to have specific employees in charge of coordinating the information security program. Any risks to consumer information must be identified by the company and the plan should be evaluated for effectiveness. If circumstances change, the program must be evaluated and adjusted accordingly. In addition, third-party service providers should be required to also maintain the appropriate safeguards.

With GLBA, there is no cookie-cutter, one-size fits all data security plan. According to the FTC, the law's requirements are purposefully flexible to allow each company to implement an information security plan that makes sense with the company's size and activities. For example, while a smaller company may have a single information security policy document and one employee to oversee it, a larger company could have multiple policy documents that set forth a procedure that is overseen by a number of employees. Moreover, the risk each company faces may be different, so it is important for companies to assess their own, individual risks, and implement a security plan accordingly.

The GLBA also requires disaster recovery and breach recovery plans. This is critical because if a lender asks to see these plans, your company needs to have them in place. These types of recovery plans cannot be developed in a day. **Drafting a viable recovery plan requires a thorough analysis of your systems by someone with IT expertise**. You need to be certain that the plan makes sense for your company and that it can be immediately implemented if a breach does occur.

The FTC states that companies must ensure that consumer information is protected in all areas of operation. However, there are three areas that are most critical: the training and management of employees, information systems, and detecting and managing breaches and system failures. These areas require special attention to ensure that consumer information is fully protected, employees are following policies and procedures, and that any breaches are discovered and consumers are notified.

The Privacy Rule focuses more on the purposeful sharing of consumer information. The rule requires financial institutions to provide their customers (and some other consumers) with a written notice that describes their privacy policies and procedures. The notice must be "clear and conspicuous."

LEGAL COMPLIANCE IS IMPORTANT

The FTC has the power to enforce violations of it GLBA rules by filing legal actions in federal district court, where it can seek injunctions and monetary damages. In most cases, state attorneys general can bring a legal cause of action in state court for violations of data security laws. A lawsuit for compliance violations is the last thing any settlement services company wants to deal with, so it is important to have knowledge of, and follow, any laws pertaining to your business.

ALTA Best Practices certification is important, and it should include a thorough analysis of your IT security posture including internal and external vulnerability assessments, a GLBA Gap analysis, penetration testing and more.

Companies like Security Compliance Associates (SCA) offer both ALTA best practices certification and analysis of legal compliance. The IT and security compliance experts at SCA keep up to date with rules promulgated by multiple federal agencies, including the FTC, Consumer Financial Protection Bureau and the Federal Financial Institutions Examination Council, and ensure that your business is compliant.

Security Compliance Associates
2727 Ulmerton Rd, Suite 310, Clearwater, FL 33762 / 1-877-993-4472 / www.scasecurity.com

WHAT DOES GLBA REQUIRE?

There is no question that certifying your best practices is very important for the title industry. However, without a systems review by a trained professional like a Certified Information Systems Security Professional (CISSP), you might leave your company at risk.

"ALTA has removed the requirement for encryption of data at rest from their assessment checklist; however, GLBA requires the safeguarding of NPI and encryption is a key security component. If you rely on only the ALTA assessment guidelines, you could be missing key components of the GLBA because it is not all encompassing of the federal requirements," said Froning.

Certifying firms need to have the expertise to review your IT infrastructure and cyber security. They need to be conducting penetration tests, phishing tests, gap analysis, and risk evaluations. They need to assess your disaster and breach recovery plans. Offsite servers, access to cloud information, firewalls, and latest system updates also need to be analyzed. Certifying firms should not simply provide you with a gap analysis. They should also have the expertise required to offer recommendations to fix issues that are discovered during an evaluation.

"Often times, companies offering certification are looking just at written policies and procedures, but they need to be taking a much closer look at security and actual practices," Froning said. "You need an IT security assessment team to come in to conduct a review of your IT infrastructure, which includes asking the following questions:

- Have you performed a penetration test? How often?
- Do you have a disaster recovery plan?
- Do you have a Data Breach Plan?
- Have your disaster recovery plan and a data breach plan been reviewed by an IT professional?
- Who manages these plans?
- Are you certain the written policies are being put into practice?

These are all issues that need to be assessed."

A thorough Pillar 3 analysis should ensure that written policies and procedures are being followed. Consider, for example, your company's security policy. Do you have one in place? What does it include? A certifying company may come in, read through your policy, and say you are certified. However, actual practices need to be taken into consideration. If there is a written policy requiring new passwords every six months, are employees truly changing their passwords as required? How is that being managed?

As another example, suppose your company has a policy requiring all employees to have antivirus on their computers. If that antivirus is not configured correctly, employees might be able to disable it because the antivirus scans slow the computers down. If that happens, and financial malware enters your system, your business could have a negligence issue. A company offering to certify your business needs to take a closer look and make sure not only that the policy is in place, but that your IT system is configured so that employees cannot disable protective measures you have put in place.

This type of assessment requires an understanding from the information security side. The best option for this type of in-depth IT security analysis is hiring an information security company. For Pillar No. 3 certification and GLBA compliance, analysis by an IT professional is critical.

To learn more about GLBA compliance and mitigating your security risks, we invite you to speak to one of the Information Security experts at Security Compliance Associates: ***877-993-4472***

ABOUT SCA

Security Compliance Associates has more than 16 years of experience delivering world class IT Information Security Assessment services throughout the United States. SCA employs credentialed engineers and compliance professionals to meet clients' IT Information Security needs. SCA Engineers have more than 100 years of combined IT and Information Security experience, including NASA Mission Operations at Johnson Space Center, the Department of Defense and the National Intelligence Community. SCA's credentialed security experts are recognized industry leaders, are frequent speakers and considered subject matter experts in the settlement, financial services and healthcare industries.

ABOUT *CERTIFICATION+*

Certification+ brings together the American Land Title Association's industry-standard Best Practices with the same information security standards adopted by lenders. Your organization can benefit from the combined services of three ALTA Elite Providers: PYA, Security Compliance Associates, and Real Estate Data Shield, uniting to provide this seamless solution. *Certification+* couples award-winning employee training with the leading industry experts on ALTA Best Practices and the Gramm-Leach-Bliley Act (GLBA) requirements.

Certification+ | PYA Certified Public Accountants | SCA Security Compliance Associates | Real Estate Data Shield™

Security Compliance Associates
2727 Ulmerton Rd, Suite 310, Clearwater, FL 33762 / 1-877-993-4472 / www.scasecurity.com

SCA