FTC SAFEGUARDS GUIDE

Whitepaper

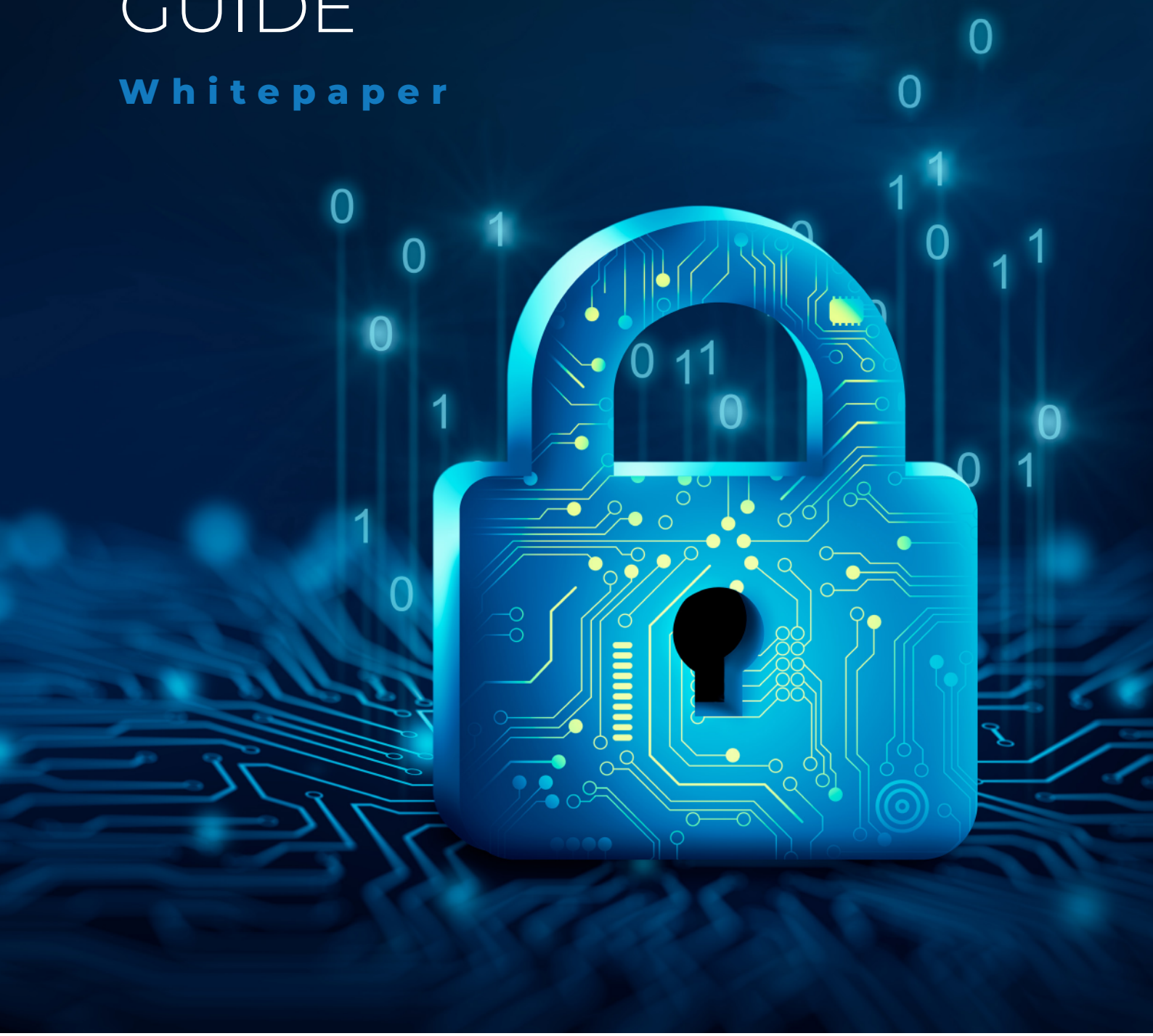


TABLE OF CONTENTS

What is Happening?

There are significant changes coming in June this year from the Federal Trade Commission that can affect your company.

As you may know, the FTC enforces a variety of federal laws related to consumer protection. Their goal is to promote competition and protect consumers' interests by enforcing laws that prohibit unfair and deceptive business practices.

Before you write this off as a "that doesn't sound like my business", there are new FTC Safeguards coming in June that define a need for compliance for security measures for your customers. They also hold a $46,000 per day per violation potential fine, with heightened enforcement.

So, without the knowledge of and compliance with these new measures, your company could be sitting in some significant hot water.

A Brief History

Way back in 1999, in response to the increased sharing of consumer information among financial institutions and the growing concern about the privacy and security of that information, the government put together the Graham-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999.

It's a federal law to protect consumers' personal financial information held by financial institutions and outlined the ways financial organizations had to comply with security protections and disclosure requirements of the customer data.

Overall, the law helped somewhat by increasing transparency and security of personal financial information, but people feel there are stark issues:

Antiquated Coverage:

The GLBA is based on 1999 technology, which obviously makes it mostly obsolete in 2023.

Lack of Clarity:

Some argue that the GLBA is not specific enough in its requirements, which can make it difficult for financial institutions to understand and comply with the law.

Scope of Coverage:

The GLBA only applies to certain financial institutions, such as banks, credit unions, and securities firms. Other types of companies that collect and use personal financial information, such as data brokers and technology companies, are not covered by the GLBA.

Minimal Consequences:

If companies didn't follow it, there wasn't a real issue as it wasn't strictly enforced by the FTC, and the penalties for violating the GLBA are relatively small, leaving some critics to argue that they are not sufficient to deter violations of the law.

Importance

Aside from alleviating the consequences that are tied into laws such as the GLBA and FTC Safeguards, which can result in significant fines if not followed correctly, there are other business reasons this is important and requires your focus.

Reputation:

A data breach or other security incident that results in the loss or theft of customer data can damage a company's reputation and erode customer trust. This can lead to a loss of customers, revenue, and overall business value.

> In fact, **55% of people in the U.S.** would be less likely to continue doing business with companies that are breached.

Competitive advantage:

A business that is perceived as taking the necessary steps to protect customer data is more likely to attract and retain customers, as well as attract and retain a talented workforce.

> Actually, **51% of small businesses** have no cybersecurity measures in place at all. Talk about a competitive advantage opportunity.

Legal liability:

A business that fails to properly protect customer data can be held liable for any resulting damages, such as identity theft or financial loss. This can lead to costly legal disputes and settlements.

Ethical responsibility:

Protecting customer data is not only important from a legal and business perspective, but it is also an ethical responsibility. Businesses have a duty to respect and protect the personal information of their customers.

Why There's a Need for Change

We've had some groundbreaking data breaches under the GLBA, which aligns with the lack of efficacy of the law.

The 2008 Heartland Payment Systems data breach was one of the most significant data breaches in history. The breach, which was discovered in January 2009, resulted in the theft of more than 130 million credit and debit card numbers, causing significant financial losses for both consumers and the company. The perpetrators used a complex network of compromised computers to gain access to Heartland's network and steal the sensitive data. The incident had a significant impact on the payments industry, leading to increased security measures and regulations to protect consumer data. The incident also resulted in significant legal actions and fines for the company, and it serves as a cautionary tale for businesses about the importance of data security and the consequences of neglecting it.

The 2013 Experian data breach was a major incident that affected 200 million consumers. The breach occurred when a hacker accessed Experian's servers and obtained personal information, including Social Security numbers, birth dates, and addresses of 15 million consumers. This information was then sold on the black market, putting consumers at risk of identity theft and other forms of fraud. The incident had a significant impact on the credit reporting industry, highlighting the need for stronger security measures and regulations to protect consumer data. Consumers were left in a state of uncertainty, had to take steps to protect themselves, such as freezing their credit, and had to closely monitor their credit reports for any suspicious activity. It highlighted the responsibility of companies that handle sensitive personal data of consumers to ensure they have proper measures in place to protect it.

The 2019 First American Financial Corp data breach was a major incident that exposed sensitive personal information of millions of consumers. The breach occurred due to a flaw in the company's website, which allowed anyone with a web browser to access more than 885 million documents containing personal information, including Social Security numbers, bank account numbers, and tax records. The incident had a significant impact on consumer privacy and security, as the exposed data could be used for identity theft and other forms of fraud.

The incident also raised concerns about the security practices of real estate companies, and the way they handle sensitive personal information of consumers. As a result of the incident, First American faced multiple class action lawsuits and fines from regulatory bodies. Additionally, consumers had to take steps to protect themselves, such as monitoring their credit reports and financial accounts for suspicious activity. The incident serves as a reminder of the importance of data security and the consequences of neglecting it.

In addition to these widespread breaches, you can see the issues with data security firsthand in a lot of company types.

Auto Dealers

- The same level of consumer data as a bank
- High turnover rate for employees
- Employees are trained in sales, not security... with decisions being made quickly so they're probably not following security rules
- They have very thin margins, so they skimp on security costs
- They are easy hacking targets
- Usually the hardware is old (ie that printer from the 90s) with little to no security

Small Accounting & Finance Firms

- Limited resources to invest in data security measures
- Lack of technical expertise to implement and maintain robust data security measures
- Difficulty in keeping up with the constantly changing data protection regulations
- No dedicated IT team or outsourced IT support, which can make it difficult to implement and maintain data security measures.
- Over-prioritization of accounting/finance tasks over data security, leading to neglect

In addition to the internal issues across diverse company types, with the major tech changes since the GBLA was put into law in 2022, something new is needed to protect your business and your consumers.

2 Huge Changes that Will Affect You

So, in December of 2021, the FTC decided to update their safeguard rules. Here's a quick rundown of the two main areas that will affect you in June.

"Financial Institution" Expansion

The FTC has drastically expanded the definition of a "financial institution". By focusing on "the types of activities" a business engages in, the rule captures businesses "significantly engaged in financial activities."

The new definition includes a broader range of companies, such as non-bank financial companies, that offer or provide financial products or services to consumers. This includes companies that offer loans, debt relief services, and credit counseling, as well as companies that provide payment processing services or store consumer financial information.

Here's a non-exhaustive list of some of the possible company types:

- Finance Companies
- Accountants
- Mortgage Lenders
- Mortgage Brokers
- Auto Dealerships
- Pay Day Lenders
- Account Servicers
- Tax prep firms
- Real Estate Appraisers
- Check cashers
- Wire transfer providers
- Loan providers - ie. a furniture company that provides a loan
- Some Travel agencies
- Career counselors
- Collection agencies
- Credit Counselors
- Non-federally insured credit unions
- Some investment advisors
- Transaction finder companies - bring buyers and sellers together

The expansion of the definition of a "financial institution" under the FTC Safeguard law is intended to provide greater protection for consumers by subjecting a wider range of companies to the law's data security and information sharing requirements. This means that a much broader range of companies will be held accountable for protecting consumer data and will be required to implement robust data security measures and comply with the FTC's regulations.

Enhanced Requirements to Comply

The new FTC Safeguard law expands upon the requirements of the GLBA by including 9 specific requirements for “financial institutions” to protect consumer data.

The 9 requirements cover areas such as risk assessment, data encryption, employee training, and incident response planning.

Businesses that fall under the expanded definition of a “financial institution” will be required to comply with these new requirements and may need to make significant changes to their current data security practices in order to do so. This will likely involve a significant investment in time and resources, and may also involve changes to the way you collect, store, and share consumer data.

Here's a breakdown of the 9 requirements, along with an option to comply with each:

1. Designate a Qualified Individual to supervise your information security program.

- The supervision of the program needs to be internal, but implementation and guidance can come from an external provider
- They are the ones responsible for FTC Safeguard compliance

ANAX Solution:

We assist a designated staff member of your company with recommendations and the implementation of a program guiding your company to compliance.

2. Conduct & Document Risk Assessments

- Determine your risk criteria
- Assess against existing controls
- Determine how those risks will be mitigated or accepted
- Conduct periodic assessments

ANAX Solution:

ANAX can assist you with the risk assessment, including a scan run across your entire infrastructure to determine where PII is stored on your network and document foreseeable risks (ie. malware, breach from a bad actor).

3. Apply Your Chosen Controls

There are 3 types: physical controls (ie. locks etc), technical controls (ie. anti-virus, encryption), and admin controls (ie. policies/ procedures). Some examples of areas you should consider:

- Apply authorized access controls
- Apply encryption of customer info
- Apply Multi-Factor Authentication (MFA)
- Apply data disposal policies
- Apply change management procedures
- Apply logging/monitoring of these controls

ANAX Solution:

We provide all the necessary controls to both comply with the new requirements, as well as cover your business from a security perspective. This includes documenting where data is stored, and if it contains PII, access management policies, legacy user assessment, encryption implementation, company-wide MFA, proper documentation of all assets, plus more.

4. Validate Your Controls

- Testing and monitoring control efficacy
- Perform continuous monitoring
- Penetration tests and vulnerability scans

ANAX Solution:

In order to continue the highest level of protection, ANAX conducts continuous monitoring and periodic penetration testing and vulnerability assessments.

5. Develop Training and Auditing Program

- Security Awareness training
- Maintain staffing for security program
- Continuing education for security

ANAX Solution:

ANAX provides continuing comprehensive training, auditing, and logging to make sure your employees understand the mechanisms of spam, phishing, spear phishing, malware, ransomware and social engineering and can apply this knowledge in their day-to-day job.

6. Monitor Service Providers

- Engage capable service providers
- Ensure security provider safeguards are codified contractually
- Perform periodic service provider reviews

ANAX Solution:

ANAX only engages the top service providers after rigorous reviews. We repeatedly ensure all vendors meet security levels that go above and beyond the FTC Safeguards.

7. Develop a Continuous Improvement Cadence

- Review risk assessments and adjust controls accordingly
- Re-evaluate security plan alongside business changes

ANAX Solution:

This is fully baked into our services as our monitoring and risk assessment cadence defines the control updates and security awareness training updates we put into place.

8. Document your Incident Response Plan

- Include goals
- Internal processes
- Well-defined internal roles for team
- Communication channels for team and org
- Remediation requirements
- Reporting criteria and processes - how to communicate during event and how to report to upper mgmt
- Review response plan after every incident

ANAX Solution:

ANAX can provide a written incident response plan designed to respond to, and recover from, any security event materially affecting your customer information.

9. Provide Annual Reporting to Senior Leadership

Reporting should include:

- Security program status
- Risk assessment findings
- Controls implemented
- Service provider engagements
- Testing results
- Security events

ANAX Solution:

ANAX will provide comprehensive reports for your senior leadership, outlining the important elements of your security program.

As you can see, there is a lot that goes into this program. All of the compliance requirements need resources such as time, money and expertise. Additionally, you may have to hire additional staff or contract specialists in order to meet these requirements.

The cost of not complying with the new FTC Safeguards can be high, as companies face fines, legal action and loss of reputation in the case of non-compliance. Therefore, it's important for companies to consider the resource needs and budget to comply with the new FTC Safeguards.

Enforcement

One of the main areas that was a drawback of GLBA was the lack of enforcement. Basically, not many companies worried about the law as there was limited enforcement of the law.

The enforcement of the new FTC Safeguards law is going to be reactive in nature, meaning that the Federal Trade Commission (FTC) primarily takes action in response to a data breach or other security incident.

This reactive enforcement approach can have some drawbacks, as it may not necessarily catch potential vulnerabilities or security issues before they lead to a data breach. So, the responsibility is yours to comply in order to make sure there are no consequences for your company.

Dependent on your current feeling on cybersecurity, you may need to shift your thinking about cybersecurity preparedness from being a “nice-to-have” to a “must-have” in order to protect your company and your customers.

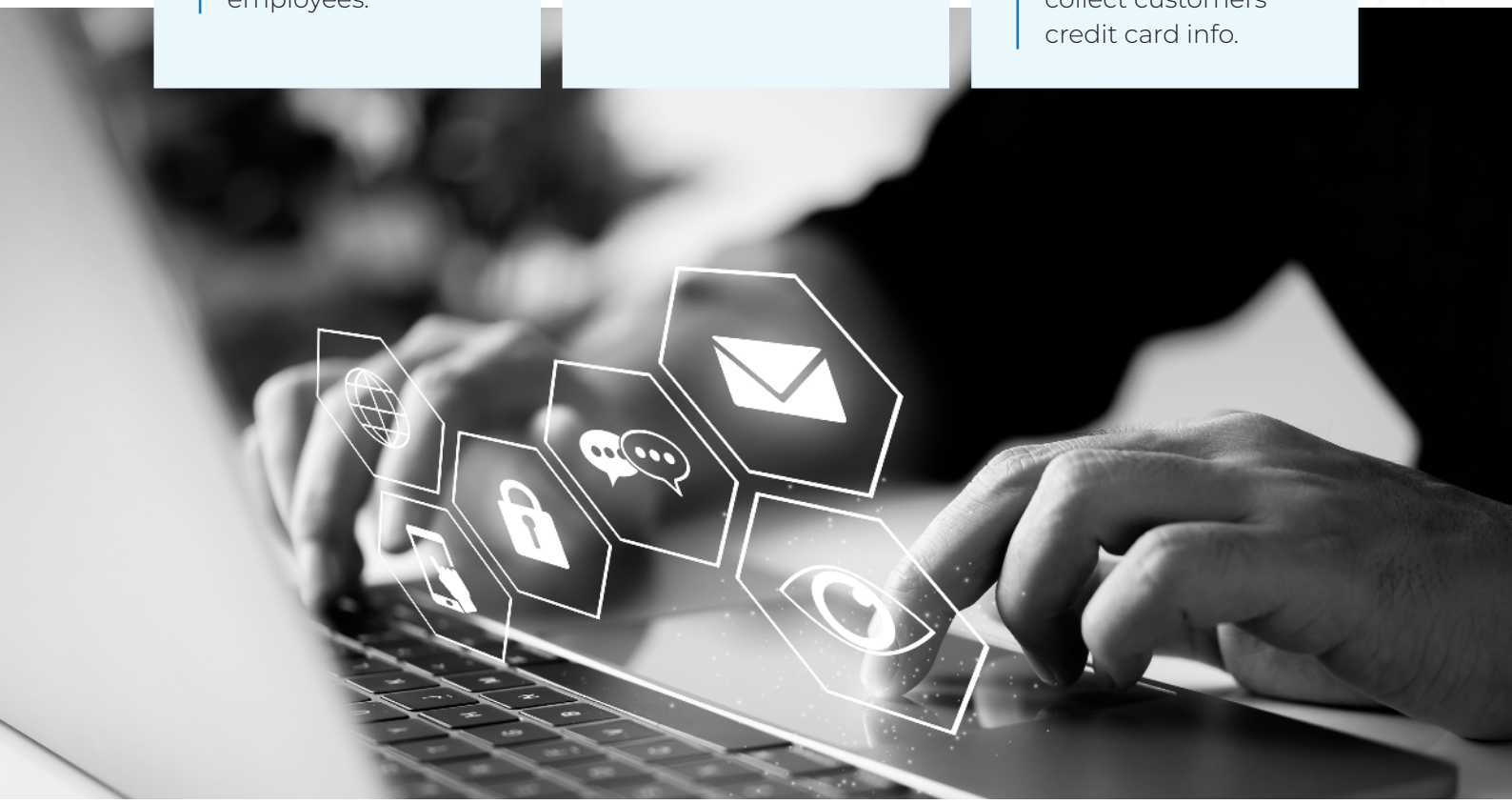
In the past, many SMBs may have viewed cybersecurity as a cost or an inconvenience, but with the increasing frequency and severity of data breaches, plus the expanded enforcement and consequences of the new FTC Safeguards, it’s becoming clear that the cost of not being prepared can be much higher.

Here are some eye-opening stats to showcase the need for your company to make this a priority:

46% of all cyber breaches impact businesses with fewer than 1,000 employees.

61% of SMBs were the target of a Cyberattack in 2021.

27% of small businesses with no cybersecurity protections at all collect customers' credit card info.



In short, you need to adopt a proactive approach to cybersecurity and understand that it's not just about complying with regulations, but about protecting your business and the trust of their customers. Yes, this will be enforced by the FTC and the Consumer Financial Protection Bureau (CFPB), but you should see it as an investment that is needed to stay competitive and to secure your company's future.

New Consequences

There are significant new consequences that accompany data breaches and a lack of compliance. Fines and penalties can be imposed by the FTC for non-compliance with the law's requirements.

The fines for non-compliance with the FTC Safeguards can vary depending on the specific circumstances of the case, such as the nature of the violation, the extent of consumer harm, and the size of the business. Although the official word is it "dependas on the case", the FTC has the authority to impose penalties up to $46,000 per day per violation.

It is also possible for individuals to face jail time for a significant or reckless disregard for the safety and security of personal information. Under the FTC Safeguards, your company and employees could face penalties and jail time if they are found to have acted with gross negligence in failing to protect consumer data.

In addition to the fines, companies that fail to comply with the FTC Safeguards may also face legal action from customers or regulatory bodies, and may be required to take steps to address and resolve data breaches, such as providing credit monitoring for affected customers, and costs associated with restoring the company's reputation.

Timeline

Originally, the new law was supposed to go into effect in December of 2022, but that got pushed back due to a number of issues including a shortage of qualified personnel to implement information security programs, supply chain issues potentially leading to delays in obtaining necessary equipment for upgrading security systems, and of course the COVID-19 pandemic.

The new date for your compliance has been moved to June 9, 2023, so it gives you a short runway to comply with the 9 areas detailed in this guide.

Options for Compliance Coverage

So, what are your next steps? You really have two options for covering these necessary changes to your security.

1. Internal coverage

You can undertake the steps to comply with the law internally. This could include:

Hiring new staff: You may need to hire additional staff with expertise in data security, such as security analysts, to help them implement and maintain robust data security measures.

Investing in technology: You may need to invest in technology such as firewalls, intrusion detection/prevention systems, and data encryption to protect customer data.

Providing employee training: You will need to provide regular employee training on data security best practices, as well as on the requirements of the FTC Safeguards and other data protection regulations.

Plus figuring out coverage of the other aspects of the 9 requirements for complying.

2. Get assistance from ANAX Business Technology

There are several reasons why you could benefit from partnering with ANAX to help you comply with the new FTC Safeguards and to protect consumer data. Some of these reasons include:

Expertise: ANAX specializes in providing IT services and support, including data security. We have the expertise and resources to help you implement and maintain robust data security measures, such as firewalls, intrusion detection/ prevention systems, and data encryption.

Compliance: ANAX is well-versed in these regulations and can help you meet the necessary requirements without any questioning if you're covered.

Proactive monitoring: ANAX can provide proactive monitoring and maintenance of your data security, which can help you respond quickly to potential threats and minimize damage if a data breach occurs.

Cost-effective: Outsourcing to ANAX can provide you with the expertise and resources needed to protect consumer data at a lower cost than hiring and training employees in-house.

Scalability: ANAX can scale our services to meet the changing needs of your business, which allows you to have the necessary cybersecurity measures in place, without having to invest in a large IT department.

In summary, partnering with ANAX Business Technology can provide you with the expertise, resources, and proactive monitoring needed to protect your consumer's data and stay compliant with regulations. It can also provide a cost-effective solution if you don't have the resources or expertise to handle data security and compliance with the new FTC Safeguards law in-house.

We're here to help with any aspects of your FTC Safeguards Compliance

Contact Us

support@anaxtech.com

(702) 478-9000

ANAX Business Technology
8920 W Tropicana Ave #104
Las Vegas, NV 89147