The 5 Biggest Mistakes Companies Are Making with the FTC Safeguards Rule and **What You Can Do to Avoid Them**

Your identity has been stolen. They applied for a credit card *in your name*. They've already gotten a new driver's license and changed your primary address to a P.O. box in a different state.

With just your Social Security Number, they were able to easily get approved for a loan and two shiny new credit cards within 24 hours of submitting the applications.

Over the course of the next three months, they max out the cards and default on the loans. You are still blissfully ignorant that there is even a problem.

Until one day, you decide to refinance your mortgage, and to your surprise,
your refinance was denied.

Months later, when you file your taxes, your accountant reports that someone has falsely filed and received a huge tax return in your name.

Now, creditors are coming out of the woodwork with their hands out, expecting to get paid. They are relentless. Phone calls day and night. Some of them are *threatening legal action*. You have no idea what to do or how to clear your name. Your credit is so damaged, you can't finance a sandwich.

Oh, and the IRS wants to *audit you* because of the fraudulent tax return they filed.

Can you imagine? You did everything right.
How could that story have such a bleak ending?

People who you trusted with your information weren't prepared, and when the title company you picked while buying your house *was hacked*, **you suffered the consequences.** It turns out your title company didn't do much to protect your data. They were focused on the deal going through but weren't really thinking about the security of your personal information.

They didn't even let you know it happened.

You found out well after the event, after the damage was done. By the time you were able to trace the problem back to the title company, your personal information has traveled across every corner of the dark web, and your financial reputation is in shambles.

It will take years, *at the very least,* to get everything back to where you started.
It's an uphill battle, draining your focus and energy.

What happened to you is happening **all too often**. Organizations are cutting corners with people's personal information, and hackers are getting their hands on and abusing this sensitive information.

This is bad for consumers, bad for business, and bad for the economy.

You might be asking, why isn't the government doing something about this? They are, but regulation lags behind technology.

40 years ago: If this were a bank robbery, the robbers would be sent to jail, and you would have your money back. Today, your financial identity is much harder to pin down.

30 years ago: Congress attempted to do something with the Gramm-Leach-Bliley Act (GLBA). However, technology is constantly changing—think about your cell phone 20 years ago—you probably could text and call. Now you could run your entire life—calendar, bank accounts, email, you name it—right on your mobile phone.

The laws simply aren't keeping up and businesses are left in the Wild West, no order and no accountability, so you—the consumer—are the one having to foot the bill.

Is that fair?

Hold onto that feeling of dread when thinking about this happening to you personally. Now multiply it by 100. The weight is suddenly unimaginable. What about 100,000? If you were the source of the leak we discussed above, that many people could easily have been compromised, and many of them would experience that gut churning scenario you imagined above.

Does your perception of events change if you run the company that was hacked?

You didn't mean to share the information, and you certainly didn't believe this could happen to you. BUT, your business didn't address the risk.

This is the problem. When businesses fail to address their risks, they leave their **customers**, their **employees** and the long-term health of their **relationships** at risk.

Would you trust the title company which leaked your data with your next big purchase? Recommend them a new client?

When sharing the story, would you call them irresponsible with your data? You likely recognize that they were a victim of cybercrime, but as a consumer, in your eyes, they screwed up.

Luckily, The FTC—Federal Trade Commission—put together new guidelines to help address the growing gap in data security. They revamped their security requirements to **include more businesses who directly interface with consumers**.

If you work with money and keep personal information about customers on file, there's a good chance you'll fall within the new FTC Safeguards guidelines.

Imagine your business was targeted with an attack—just like that title company—and word got out that you weren't doing ***the bare minimum***—what these new standards are requiring—to protect your clients' data. These new regulations are daunting and being on the right side of them is exceptionally important. How do you make sure your company is doing what it needs to do?

The 5 biggest mistakes we see when it comes to FTC safeguards are problems with:

- Briefing senior leadership
- Oversight/Implementation
- Training programs
- Incident response plan
- Control validation

Did you know: *Getting a third-party assessment will show you if there are any holes in your security.*

Let's take a closer look at the new rules and the mistakes people are making that could put **your data** at risk.

The FTC Safeguards Rule is designed to protect the information of financial institutions' customers. Noncompliance leads to heavy fines and disruptive oversight.

The big picture:

In 1999, Congress passed a **financial reform act** (the Gramm-Leach-Bliley Act) which was supposed to modernize the financial sector. It was a huge step forward as the last major financial regulation legislation was in **1933** (the Glass-Steagall Act) to address the Great Depression. The GLBA did make some **big improvements**. It defined security protections which were necessary and appropriate for the time as well as codifying disclosure requirements.

The GLBA was a thoughtful and well-intentioned piece of legislation which, because of a combination of clarity issues and rapidly evolving technology, had **no teeth on the enforcement front**. From 1999 to 2021, over a billion sensitive records were leaked, hacked, or stolen. Clearly, something had to give.

Thus, in 2021, the FTC passed and released their new FTC Safeguards rule. One of the biggest **problems** with the GLBA was scope. In the final 2002 version of the legislation, they said:

"This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to entities such as 'you.'"

The biggest problem here is that GLBA assumed that everyone had the same definition of "financial institution" which was the Achilles heel of the entire act. Instead of arguing whether or not an institution was complying with the law, companies could argue that they didn't fit the definition of a financial institution. This made it really difficult to impose penalties (which made it a lower order priority for companies). Compare that to the 2021 version of the FTCSR:

*"**Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. Namely, this part applies to those "financial institutions" over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.** An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. **More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.** They are referred to in this part as 'You.'"*

They open with GLBA's language and then expand heavily on exactly what they mean by "financial institution" including classifying significantly more types of business as "covered entities."

So, who is considered a covered entity?

- Mortgage lenders
- "Pay day" lenders
- Finance companies
- Mortgage brokers
- Account servicers
- Check cashers
- Wire transferors
- Some travel agencies
- Real Estate appraisers
- Credit counselors
- Automotive dealerships
- Tax preparation firms
- Non-federally insured credit unions
- Some investment advisors

The unifying thread here is that all these institutions **handle both customer information and finances.**

The expansion of who is a financial institution gives the FTC stronger grounds on which to impose penalties and enforce these new requirements.

Consequences of noncompliance:

Just by being found negligent, the FTC can impose fines from **$10,000 to $100,000 per violation.** That total amount is at the discretion of the individual regulator, so it is difficult to say how high any single fine will be.

In addition, if you're found to be in gross violation of the rule, you can get up to **5 years in prison**. Now, that last one only really applies to things like intentional abuse of protected information, but the FTC is making a clear case that their new teeth are sharp, and they are not afraid to use them.

Importantly, the FTC is going to be reactive rather than proactive. This means that regulators will come to your business and examine every square inch of your security program with a microscope **after you've had an incident.**

Scenario: You've been hit with a ransomware attack

Your backups have been deleted. Your data has been encrypted down to the last bit. You're having to negotiate a ransom in cryptocurrency to get back access to your information. If you don't get that data back, your company is ruined. While this is happening, you have to explain to your stakeholders what happened. You have to keep your staff from panicking. Investors are getting skittish.

On top of all of that, you're answering regulator questions and paying out fines while trying to recover from the event. You'll also lose crucial time that you need to get your services back on their feet. Estimates vary, but the average data breach costs between from **$3-5 million**, and that doesn't include the much more difficult to calculate losses that come from **reputation damage**. The first thing your insurance adjustor will ask is whether or not you're compliant, and if you're not, any claims could be denied.

Okay, you're sufficiently invested in why these new regulations are important, so how can your company stay on the right side of them?

These regulations are serious*: Want to be sure that you stay on the right side of these regulations, contact us to schedule a Level 1 Assessment.*

These are the exact worst-case-scenarios that a third-party assessment can help prevent.

In the meantime, these five pitfalls are what we recommend you be on the lookout for.

5 big mistakes (and how to avoid them)

Mistake #1: Senior leadership isn't in the loop

Surely this couldn't happen to your company though. Right? After all, you have a good IT person/staff. But how do you know? Unless your company is in the information technology sector, there's a good chance your senior leadership doesn't know what goes into keeping an IT department running, much less what it takes to stay FTC compliant. That's changing. The new regulations require company leadership to receive r**eports on your security program status** including:

- **Assessments:** This means having a qualified expert find all the holes in your security (and if you don't do regular third-party assessments, there very likely are holes).
- **Improvement recommendations**: You know what is wrong, and that's a great step one. But now you need to know what your company plans to do to address it.
- **Incident reports:** When something goes wrong, senior leadership needs to be briefed on incidents and kept apprised of how they are being addressed.

Back to that ransomware attack: How would you learn that hackers are holding your whole infrastructure hostage? When would you learn that it happened? Hopefully before you're approached by a reporter on your way out of the office. Now, your company is making front page news, and the headlines are not flattering.

What can you do? Take a vested interest in your security:

You're already reading this report, so let's assume we've got buy-in. Great! Now is the time to get to know what your security program looks like. Ask questions. Don't get bowled over by jargon. If it doesn't make sense, keep pressing for more information until it does. This starts in the C-suite and works down through every part of the company.

Remember, if anything goes wrong, it might be *you* giving a press conference and having to answer the tough questions.

Mistake #2: Oversight/implementation of your security program got neglected

Maybe you didn't **designate a qualified individual,** or you assumed **designating someone outside your organization** keeps you off the hook. Either way, as the business owner, **you're responsible** for your organization's compliance.

There isn't much of a definition of a "qualified individual" in the rule. This is a double-edged sword. It's easy enough to make a case that your security person is qualified. By the letter of the rule, your IT person would be okay. However, the FTC giving leeway with who can run your security program does not equate to getting leeway with how well your program functions.

Couldn't the IT department handle it then?

The short answer: They aren't equipped to handle this *in addition* to the litany of other responsibilities they have. On a given day, IT is keeping a hundred plates spinning to keep your hardware and software running smoothly. By definition, they have to function as generalists. Do you think there is time in their schedules to keep up with the ever-changing landscape of security?

Would you bet your reputation on it?

We are focused on security. It's our bread and butter. We're looking for the next big vulnerability before it crashes your systems. Our job isn't to put your employees out of a job. It's to make sure that all their hard work doesn't go up in smoke when a hacker picks your company as their next target.

You cannot proofread your own work

Think about the last time you got on an airplane. The pilot goes through a preflight checklist and confirms it with the tower. The pilot is double-checking to make sure that everything that was done by other people is done correctly. Very likely, you get some comfort knowing that someone is maintaining the plane, fixing problems, and looking for flaws. It's even more comforting that an objective third party is double checking that work. The same holds true for security. Your people know what they're doing, but they also know what *should be there* when examining your system. That leads to inattentional blindness, the kind that an extra pair of eyes will catch.

Mistake #3: Your training program is nonexistent or insufficient

The FTC REQUIRES you to implement a training program. It **must** teach your employees the latest tricks that hackers are using to get in. You could build a program from scratch and update it with each new development in the security space (see Mistake #2 and ask if that's the right way to go). On top of that, you have to ensure your employees understand the material (*and document it)*.

How can you handle this?

Get your training materials from subject matter experts. In the same way a specialist can help build your security program, a specialist can educate how to keep your data safe. Around 70% of all data leaks (though some sources put it as high as 90%) come from social engineering. That puts you in a place where every single person in your company has to be the first line of defense against hackers.

Not everyone has access to sensitive data

That's true, but if one employee is hacked, there's a wedge in the door. Suddenly, phishing attempts are coming from that unwitting employee, and the hackers can use this as a beachhead to get more information. Essentially, you're only as strong as your weakest link, and you cannot afford for it to be your security training program.

Mistake #4: You haven't set up your incident response plan

Back to your hypothetical ransomware problem: Can you imagine answering tough questions about how an incident occurs without so much as a briefing to prepare yourself? When an event occurs, you want to project strength. You know exactly how it happened and are already taking steps to mitigate it. You **can't** "just figure it out" after you've been hacked. Remember, all of the disaster of a breach (the bad press, the FTC investigation, dealing with hackers, reputation recovery) is happening at the same time. It's already a three-ring circus. Don't let it be your lion tamer's first day on the job.

Yes, it can happen to you

Hackers are largely opportunists. They attack systems that are easy targets. If your plan is being created on the fly, they are going to extract more value from information that they steal. Think about how we secure a car. Yes, there's the door locks. That's your security program. There's also the alarm though. A big flashy noise that shortens the amount of time the thief has to make off with your car. A good incident response plan puts you in a position to respond *quickly* to an event. It limits how far they'll get in your systems, how much data they can steal, and how much money they can make off that data.

The FTC requires you to document your plan

We're way past scout's honor on having an incident response plan. When they are investigating you, the FTC wants to be sure that you did everything you could to protect that data. They want to be sure you're doing everything you can from the moment something goes wrong. If you aren't...it gets costly very quickly.

Mistake #5: You don't have a method for validating controls

Would you buy a safe that the manufacturer is "pretty sure" it'll work? Of course not. You want the safe that stumped professional safe crackers. That's because if you are bothering to buy a safe, you want its contents to remain secure. Now imagine that instead of being in your office, cleverly hidden behind a painting, the safe is in the middle of Times Square. Suddenly, that safe needs to be foolproof. Anything less than that, and it's a deterrent, not a defense.

That's your data

Everything that we do: Encryption, password protection, biometrics, multi-factor authentication; it's all security features for the digital equivalent of a safe in Times Square. That's why validating your controls is important. If you don't, you'll find out there's a problem on Monday when the safe door is blown off and you have to walk through police tape to get in the front door.

You have to test your controls

This isn't just a smart thing to do. It's **legally required** under the FTC safeguards rule. Now, you could try to verify in-house (see Mistake #2 for why you shouldn't). However, you've seen how complicated all of this is. You know that there are a multitude of sensitive, moving pieces at play to make sure your security plan is up to snuff.

Put another way:

You're (hopefully) starting to see the value in third party **penetration testing** and **vulnerability analysis**. There isn't room for this increasingly common problem to happen to you. We can help get you from where you are to where you need to be.

What can we do to help?

You're legally obligated to have a risk mitigation strategy. Shouldn't you go into it with open eyes?

I want to offer you a Level 1 Risk Assessment.

This isn't a tool that you're left to figure out. Our goal is to help you understand your risks and what to do to address them.

This is a $3,000 value that I'm offering to you free of charge if you begin this process with us in the next 30 days.

You're at the center of this process:

We'll have a 45-minute call to discuss threats and risk. This is just the beginning of the process. We get to know you, and don't worry; our non-disclosure agreement means that your information remains confidential.

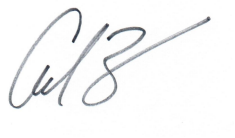
After that, we'll analyze your current processes to see where you stand with respect to the FTC requirement. After that, you and I can work together to build a roadmap to get you up to the new rule's requirements.

We won't be giving you the hard sell because this process is meant to take time. We want to help you do it right. That means the more time we have to work with you before the FTC Safeguards implementation deadline, the better (You wouldn't start your taxes in mid-April, would you?).

Here for you:

If you're ready to take the next step, call me at 208-881-9713 to schedule your meeting and get your FREE Level 1 Risk Assessment.

Dedicated to serving you,



Aaron Zimmerman
Web: www.TotalCareIT.net
email: aaronz@totalcareit.net
Direct: 208-881-9713