

Building an FTC-Compliant Information Safeguard Program: An Action Plan

General Instructions

This Action Plan is designed to help you cover all of the bases when developing an FTC-compliant customer information safeguard program. Keep in mind that one of the new provisions requires you to create a written document outlining your particular safeguard program. THIS ACTION PLAN IS **NOT** A SUBSTITUTE FOR THAT WRITTEN DOCUMENT!!!!

Think of this plan as more of a comprehensive, detailed checklist that will provide you with guidance in exploring all of the facets of your company and its treatment of customer information privacy. The finished version of this Action Plan will have all of your input and can be used as a source for generating that final official company document regarding your new customer information privacy program.

The changes you make will depend on the size of your company, what sort of physical and technological expansion you expect, and what safeguards you already have in place.

Check off the boxes next to each step when you have completed it. You may want to make a bundle of copies of this document to assist in future audits!

Step-by-Step

Step 1: Appoint a Coordinator

The first order of business when setting up a safeguard program is to appoint an employee or employees to oversee its creation and implementation. Assigning a coordinator (and, if necessary, assistants) will show your commitment to becoming compliant with the FTC rulings and protecting private customer information.

Be careful when selecting this person or these persons! They are the faces of your program for both your customers and your employees. Whether dealing with customers or other employees, your Safeguard Program Coordinator must command respect through his or her efficiency, attention to detail, accessibility, and exceptional communication skills.

If your company is larger, you may want to appoint more than one person to your coordination staff. But no matter how many people you put to work on this task, the attributes outlined above must be in place for each and every one of them.

Remember, this person or these people will be in charge of assessing your company's information privacy needs as well as any necessary employee training and support. They will be the first people that your employees go to with questions. They will be the first (and possibly the only) people your customers talk to with questions or concerns. They will be the liaison between the FTC and your company.

□ **Step 2: Separating “Customers” from “Consumers”**

The new FTC safeguard provisions apply specifically to “customer” information. Now, while “customer” and “consumer” may not sound very different to you, this new ruling actually differentiates the two terms. A “customer” is someone you have a direct dealing with, someone you have had a transaction with. That person's information is the focus of these new provisions.

A “consumer” is a person that you have an indirect relationship with. This person's information is not necessarily covered by these new provisions. You still have to make disclosures to consumers letting them know if and how they are covered by these new rulings.

After designating a Coordinator, you are going to want to separate out the “customer” information from the “consumer” information so that you can more easily assess your security system based on the information that is actually covered under the new ruling.

However, be careful when separating these two sets of information from one another! If you are unsure whether a certain person's information would be considered “customer” or “consumer”, consider it “customer” information and, therefore, protected under these new provisions! Better to be safe than to spend \$11,000 a day in fines because you were careless!

□ **Step 3: Assessing Your Current Standards**

In order to know what changes need to be made, you first have to assess your current standards for protecting private customer information.

Take a long hard look at both internal and external risks to the confidentiality and integrity of customer information. Now, you don't have to be prophetic here! Just try to assess reasonably foreseeable internal and external risks to customer information that could arise from any of the following:

- Unauthorized disclosure
- Misuse
- Alteration
- Destruction
- Or any other compromise

Once you have assessed the possible risks to customer information, analyze your current safeguards to see if those safety nets sufficiently protect customer information and satisfy the new provisions of the FTC ruling.

Think of this assessment as a ship check in which you want to make sure that the vessel is water-tight and sea-worthy. You are going to be looking at your company to be sure that customer information is locked up tight and that you are ready to go about your daily routines with those protections still in place. If you forge ahead without ensuring the integrity and confidentiality of customer information, you run the risk of racking up the now-infamous \$11,000 per day fines for violating the new rulings!

In making this assessment, take a look at:

- 1. Employee training and management**—Are your employees properly trained on the new FTC provisions for customer information privacy? Do they know when they are allowed to share consumer info and when not to? Are they being supervised properly by managers who know the new provisions thoroughly? Do those managers offer guidance to the employees?
- 2. Information systems, including:**
 - **Network design**—Is the computer network your office works with stable? Have you had any problems with it in the past? If so, were those problems fixed properly? Is the network truly secure from being cracked by hackers? Or, could a sufficiently skilled hacker access customer information rather easily?
 - **Software design**—Are the software programs you use to collect and store customer information stable? Are there bugs in the software? Can you fix those bugs through upgrades to the current programs? Or, will you have to find completely new programs to use in order to comply with the new FTC regulations?
 - **Information processing**—How is customer information your company handles processed? What procedures does the information go through—both physical and technological? Is the information secure at every stage of the processing chain? If not, is the problem a personnel

issue or a technology issue? Whose hands does this information go through? Are those people trained in the new FTC provisions?

- **Information storage**—How is the information stored? If it is stored technologically, is the storage system stable and secure? Or, does it have bugs that could make it unstable and insecure? If the information is stored in a physical location in hard copy files, are the files in a locked, secure location such as a file closet or a cabinet? How vulnerable are these storage facilities to burglary or catastrophe?
- **Information transmission**—How is information transmitted to affiliates and third party providers? Is the method of transmission secure and stable? Or, are there opportunities for outside parties to intercept the information in transit? How is information transmitted internally? Are your employees careful in handling the information when they receive it? Do they leave hard copies of files lying around? Do they leave their computer terminals unlocked when they go on a lunch break or when they go home at night?
- **Information disposal**—How does your company dispose of information? Are computer files deleted completely? Are hard copies of files thrown into the dumpster out back without being shredded or censored? Or, is there a system for shredding and recycling the documents in a secure manner?

3. **Detecting, preventing, and responding to attacks, intrusions, or other system failures**—What mechanisms are in place to find out about or prevent any sorts of failures? For example, if there is an information leak, how quickly would it be detected and corrected? If the computer system is attacked, is it strong enough to withstand a heavy hacker assault?

□ **Step 4: Fixing the Holes**

Take a look at the discoveries you made in the above assessment. Are there problems with the way your company handles customer information?

Rather than just fixing the isolated problems, though, create and implement a Safeguards Program to ensure that the information-handling and security problems are corrected within the context of a cohesive and comprehensive program.

We'll talk about maintaining the program a little later. Right now, you should develop and implement this program as soon as possible, because if the FTC comes down on you, it will come down hard—to the tune of \$11,000 a day in fines!

□ **Step 5: Scrutinizing Service Providers and Affiliates**

Now, it's time to shift your focus outwardly to the entities that provide outside services for your company and affiliates that you work with. Do your providers and affiliates have sufficient protections in place for customer information? Use the same tests and ask the same questions that you employed in investigating your own company. Don't be shy! This new FTC ruling requires you to find out about and suggest improvements to your providers' and affiliates' customer information-handling and security procedures and safeguards.

If you find that the providers and affiliates you work with do not have programs that satisfy the FTC's new ruling, then you should contractually bind those companies to create customer information protection programs. This is a must for you and for them, because it keeps both of you from being fined heavily.

In fact, even if you find that your providers and affiliates already have programs in place that satisfy the FTC's Safeguards Rule, you should still contractually require them to keep those programs maintained.

Having the contract stating that you required the affiliate to instate or maintain customer information protection programs may just save you from being dragged down with that provider or affiliate should they come under investigation by the FTC!

□ **Step 6: Monitor and Maintenance**

This step is ongoing. You should be constantly assessing the effectiveness of your information security system, possibly doing bi-annually or quarterly audits. When you do these audits, consider the same aspects and ask the same questions that we outlined in Step 3. And when you consider those aspects of your information security system, also look at recent changes in operations and technology and make sure that your system is still sound and effective with the changes in place.

Additionally, always be aware of what changes are coming for your company. What are your plans technologically for the next year? Or the next five years? How will those advances in technology affect your information security system? What about personnel? Are you going to be downsizing? How might the lack of employees affect your information security system? Would a disgruntled employee be able to circumvent your system easily? Are you going to be adding employees? Can you fully train them on the system before they begin working?

Finally, you should also be constantly aware of the changes that your providers and affiliates experience. Are they downsizing or growing? Have they adequately

maintained their information security programs? Have they been investigated for any offense related to customer information security?

There are a lot of questions here, but they (along with the ones outlined in Step 3) are extremely important in assessing your security system and its capabilities.