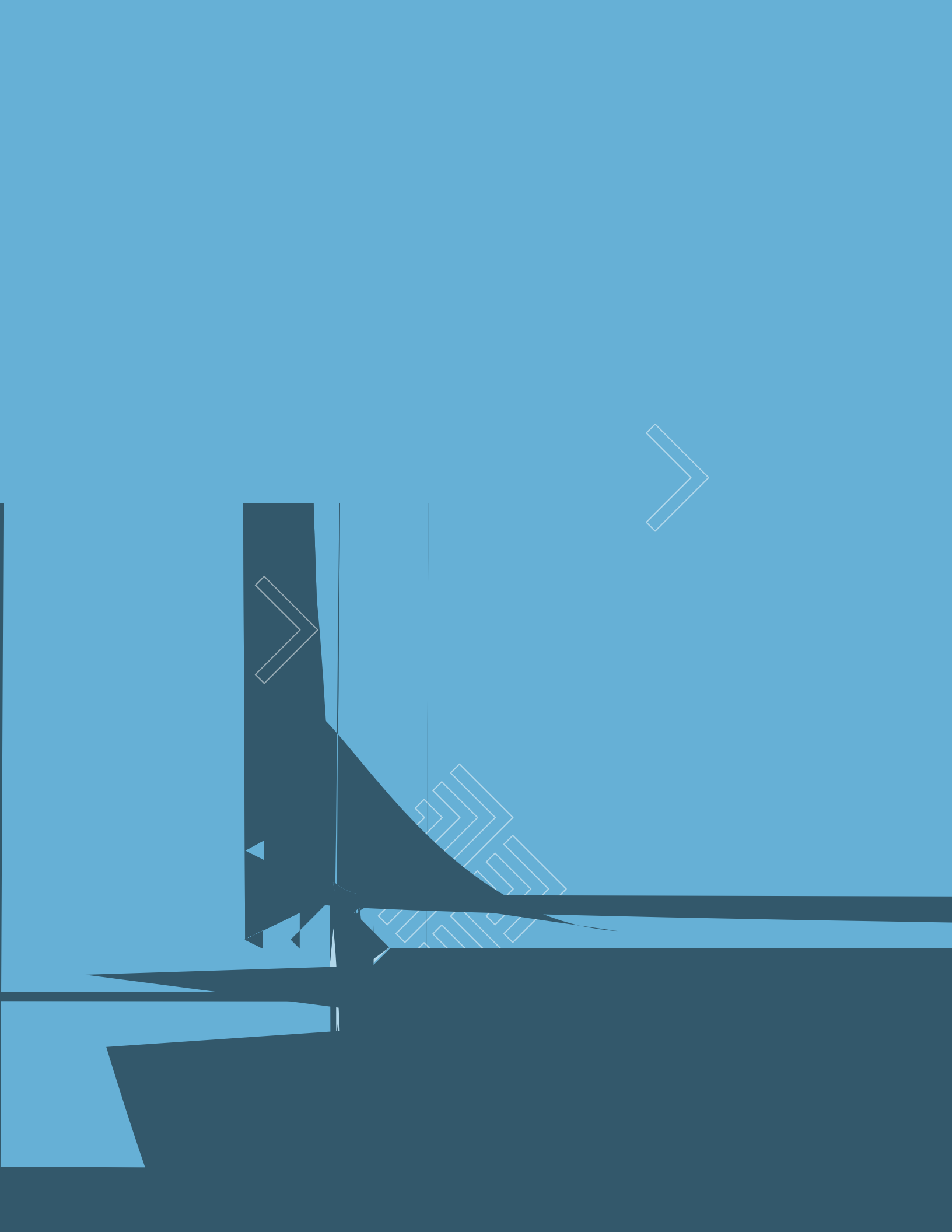
START WITH SECURITY

A GUIDE FOR BUSINESS

LESSONS LEARNED FROM FTC CASES

FEDERAL TRADE COMMISSION



START WITH SECURITY

1. **Start with security.**
2. **Control access to data sensibly.**
3. **Require secure passwords and authentication.**
4. **Store sensitive personal information securely and protect it during transmission.**
5. **Segment your network and monitor who's trying to get in and out.**
6. **Secure remote access to your network.**
7. **Apply sound security practices when developing new products.**
8. **Make sure your service providers implement reasonable security measures.**
9. **Put procedures in place to keep your security current and address vulnerabilities that may arise.**
10. **Secure paper, physical media, and devices.**

1 Start with security.

From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Business executives often ask how to manage confidential information. Experts agree on the key first step: Start with security. Factor it into the decisionmaking in every department of your business – personnel, sales, accounting, information technology, etc. Collecting and maintaining information "just because" is no longer a sound business strategy. Savvy companies think through the implication of their data decisions. By making conscious choices about the kind of information you collect, how long you keep it, and who can access it, you can reduce the risk of a data compromise down the road. Of course, all of those decisions will depend on the nature of your business. Lessons from FTC cases illustrate the benefits of building security in from the start by going lean and mean in your data collection, retention, and use policies.

Don't collect personal information you don't need.

Here's a foundational principle to inform your initial decision-making: No one can steal what you don't have. When does your company ask people for sensitive information? Perhaps when they're registering online or setting up a new account. When was the last time you looked at that process to make sure you really need everything you ask for? That's the lesson to learn from a number of FTC cases. For example, the FTC's complaint against ***RockYou*** charged that the company collected lots of information during the site registration process, including the user's email address and email password. By collecting email passwords – not something the business needed – and then storing them in clear text, the FTC said the company created an unnecessary risk to people's email accounts. The business could have avoided that risk simply by not collecting sensitive information in the first place.

Hold on to information only as long as you have a legitimate business need.

Sometimes it's necessary to collect personal data as part of a transaction. But once the deal is done, it may be unwise to keep it. In the FTC's ***BJ's Wholesale Club*** case, the company collected customers' credit and debit card information to process transactions in its retail stores. But according to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but by holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company's security practices, hackers stole the account data and used it to make counterfeit credit and debit cards. The business could have limited its risk by securely disposing of the financial information once it no longer had a legitimate need for it.

Don’t use personal information when it’s not necessary.

You wouldn’t juggle with a Ming vase. Nor should businesses use personal information in contexts that create unnecessary risks. In the ***Accretive*** case, the FTC alleged that the company used real people’s personal information in employee training sessions, and then failed to remove the information from employees’ computers after the sessions were over. Similarly, in ***foru International***, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.

2 Control access to data sensibly.

Once you’ve decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure. You’ll want to keep it from the prying eyes of outsiders, of course, but what about your own employees? Not everyone on your sta needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a “need to know” basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. For paper files, external drives, disks, etc., an access control could be as simple as a locked file cabinet. When thinking about how to control access to sensitive information in your possession, consider these lessons from FTC cases.

Restrict access to sensitive data.

If employees don’t have to use personal information as part of their job, there’s no need for them to have access to it. For example, in ***Goal Financial***, the FTC alleged that the company failed to restrict employee access to personal information stored in paper files and on its network. As a result, a group of employees transferred more than 7,000 consumer files containing sensitive information to third parties without authorization. The company could have prevented that misstep by implementing proper controls and ensuring that only authorized employees with a business need had access to people’s personal information.

Limit administrative access.

Administrative access, which allows a user to make system-wide changes to your system, should be limited to the employees tasked to do that job. In its action against ***Twitter***, for example, the FTC alleged that the company granted almost all of its employees administrative control over Twitter's system, including the ability to reset user account passwords, view users' nonpublic tweets, and send tweets on users' behalf. According to the complaint, by providing administrative access to just about everybody in-house, Twitter increased the risk that a compromise of any of its employees' credentials could result in a serious breach. How could the company have reduced that risk? By ensuring that employees' access to the system's administrative controls was tailored to their job needs.

3 Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password "hygiene" – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are tips to take from FTC cases.

Insist on complex and unique passwords.

"Passwords" like 121212 or qwerty aren't much better than no passwords at all. That's why it's wise to give some thought to the password standards you implement. In the ***Twitter*** case, for example, the company let employees use common dictionary words as administrative passwords, as well as passwords they were already using for other accounts. According to the FTC, those lax practices left Twitter's system vulnerable to hackers who used password-guessing tools, or tried passwords stolen from other services in the hope that Twitter employees used the same password to access the company's system. Twitter could have limited those risks by implementing a more secure password system – for example, by requiring employees to choose complex passwords and training them not to use the same or similar passwords for both business and personal accounts.

Store sensitive personal information securely and protect it during transmission.

For many companies, storing sensitive data is a business necessity. And even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it. Given the nature of your business, some possibilities may include Transport Layer Security/Secure Sockets Layer (TLS/SSL) encryption, data-at-rest encryption, or an iterative cryptographic hash. But regardless of the method, it's only as good as the personnel who implement it. Make sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation. With that in mind, here are a few lessons from FTC cases to consider when securing sensitive information during storage and transmission.

Keep sensitive information secure throughout its lifecycle.

Data doesn't stay in one place. That's why it's important to consider security at all stages, if transmitting information is a necessity for your business. In ***Superior Mortgage Corporation***, for example, the FTC alleged that the company used SSL encryption to secure the transmission of sensitive personal information between the customer's web browser and the business's website server. But once the information reached the server, the company's service provider decrypted it and emailed it in clear, readable text to the company's headquarters and branch o□ces. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, and not just during the initial transmission.

Use industry-tested and accepted methods.

When considering what technical standards to follow, keep in mind that experts already may have developed e□ective standards that can apply to your business. Savvy companies don't start from scratch when it isn't necessary. Instead, they take advantage of that collected wisdom. The ***ValueClick*** case illustrates that principle. According to the FTC, the company stored sensitive customer information collected through its e-commerce sites in a database that used a non-standard, proprietary form of encryption. Unlike widely-accepted encryption algorithms that are extensively tested, the complaint charged that ValueClick's method used a simple alphabetic substitution system subject to significant vulnerabilities. The company could have avoided those weaknesses by us7cantoTccn/GS0 g

Ensure proper configuration.

Encryption – even strong methods – won't protect your users if you don't configure it properly. That's one message businesses can take from the FTC's actions against ***Fandango*** and ***Credit Karma***. In those cases, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned o a critical process known as SSL certificate validation without implementing other compensating security measures. That made the apps vulnerable to man-in-the-middle attacks, which could allow hackers to decrypt sensitive information the apps transmitted. Those risks could have been prevented if the companies' implementations of SSL had been properly configured.

Segment your network and monitor who's trying to get in and out.

When designing your network, consider using tools like firewalls to segment your network, thereby limiting access between computers on your network and between your computers and the internet. Another useful safeguard: intrusion detection and prevention tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Segment your network.

Not every computer in your system needs to be able to communicate with every other one. You can help protect particularly sensitive data by housing it in a separate secure place on your network. That's a lesson from the ***DSW*** case. The FTC alleged that the company didn't su ciently limit computers from one in-store network from connecting to computers on other in-store and corporate networks. As a result, hackers could use one in-store network to connect to, and access personal information on, other in-store and corporate networks. The company could have reduced that risk by su ciently segmenting its network.

Monitor activity on your network.

“Who’s that knocking on my door?” That’s what an e□ective intrusion detection tool asks when it detects unauthorized activity on your network. In the ***Dave & Buster’s*** case, the FTC alleged that the company didn’t use an intrusion detection system and didn’t monitor system logs for suspicious activity. The FTC says something similar happened in ***Cardsystem Solutions***. The business didn’t use su□cient measures to detect unauthorized access to its network. Hackers exploited weaknesses, installing programs on the company’s network that collected stored sensitive data and sent it outside the network every four days. In each of these cases, the businesses could have reduced the risk of a data compromise or its breadth by using tools to monitor activity on their networks.

Secure remote access to your network.

Business doesn’t just happen in the o□ce. While a mobile workforce can increase productivity, it also can pose new security challenges. If you give employees, clients, or service providers remote access to your network, have you taken steps to secure those access points? FTC cases suggest some factors to consider when developing your remote access policies.

Ensure endpoint security.

Just as a chain is only as strong as its weakest link, your network security is only as strong as the weakest security on a computer with remote access to it. That’s the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For exasec(e f/GS17df)]ess[acceskcmo mon

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-

Follow platform guidelines for security.

When it comes to security, there may not be a need to reinvent the wheel. Sometimes the wisest course is to listen to the experts. In actions against ***HTC America***, ***Fandango***, and ***Credit Karma***, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned o a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for developers, which explicitly warn against turning o SSL certificate validation.

Verify that privacy and security features work.

If your software o ers a privacy or security feature, verify that the feature works as advertised. In ***TRENDnet***, for example, the FTC charged that the company failed to test that an option to make a consumer's camera feed private would, in fact, restrict access to that feed. As a result, hundreds of "private" camera feeds were publicly available. Similarly, in ***Snapchat***, the company advertised that messages would "disappear forever," but the FTC says it failed to ensure the accuracy of that claim. Among other things, the app saved video files to a location outside of the app's sandbox, making it easy to

Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to

Put procedures in place to keep your security current and address vulnerabilities that may arise.

Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to keep your guard up. If you use third-party software on your networks, or you include third-party software libraries in your applications, apply updates as they're issued. If you develop your own software, how will people let you know if they spot a vulnerability, and how will you make things right? FTC cases offer points to consider in thinking through vulnerability management.

Update and patch third-party software.

Outdated software undermines security. The solution is to update it regularly and implement third-party patches. In the ***TJX Companies*** case, for example, the FTC alleged that the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Depending on the complexity of your network or software, you may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third-party software is an important step to reducing the risk of a compromise.

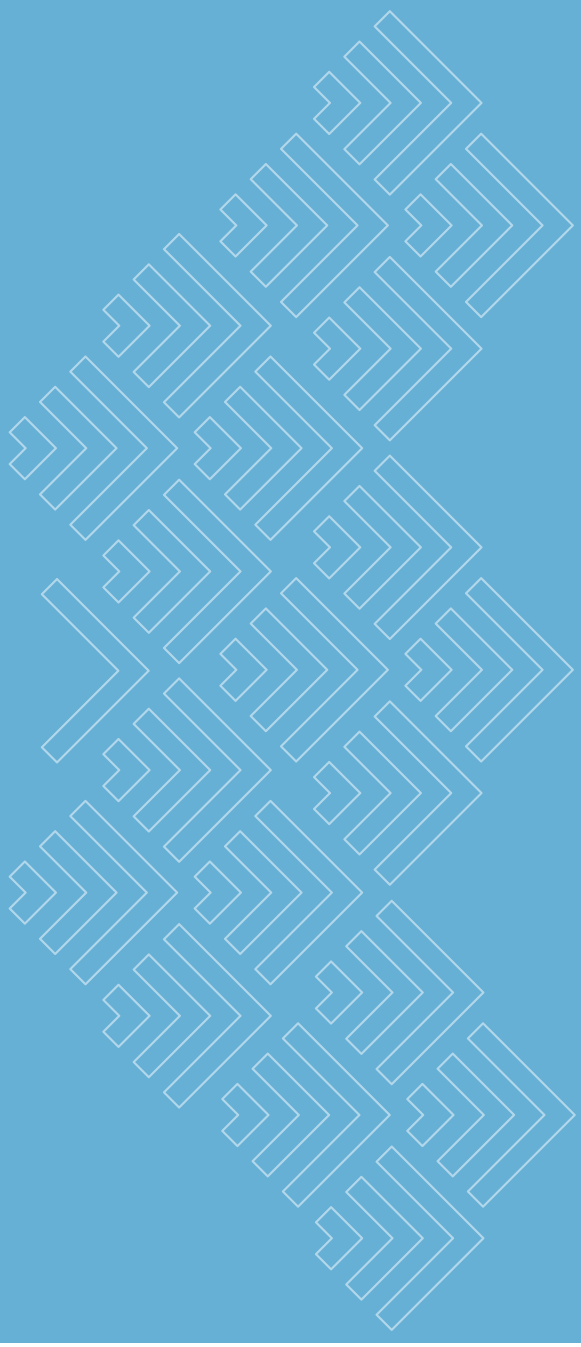
Heed credible security warnings and move quickly to fix them.

Looking for more information?

The FTC's Business Center (**business.ftc.gov**) has a Data Security section with an up-to-date listing of relevant cases and other free resources.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your



Federal Trade Commission
business.ftc.gov
June 2015