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.**

When managing your network, developing an app, or even organizing paper files, sound security is no accident. Companies that consider security from the start assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved. Threats to data may transform over time, but the fundamentals of sound security remain constant. As the Federal Trade Commission outlined in *Protecting Personal Information: A Guide for Business*, it's critical to know what personal information you have stored physically and electronically, and keep only what is essential for your business. Protect the information you keep, and properly dispose of what you no longer need. And, of course, create a plan to respond to security incidents.

The FTC also has *cybersecurity resources* especially for small businesses, including publications to address particular data security challenges, business alerts, and guidance to help you identify – and possibly prevent – pitfalls.

There's another source of information about keeping sensitive data secure: the lessons learned from the more than 80 law enforcement actions the FTC has announced so far. These are settlements – no findings have been made by a court – and the specifics of the orders apply just to those companies, of course. But learning about alleged lapses that led to law enforcement can help your company improve its practices. And most of these alleged practices involve basic, fundamental security missteps. Distilling the facts of those cases down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.

1 ▶ Start with security.

Business executives often ask how to manage confidential information ranging from personal data on employment applications to network files with customers' credit card numbers. Experts agree on the key first step: Start with security. Factor it into the decision-making 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. Instead, deliberately think through the implications of your 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. Even when information must be collected and stored, consider whether it can be stored exclusively on the user's device.

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 this 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 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 the company with giving 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 staff 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 vendors and contractors don't have to use consumers' sensitive personal information as part of their services, there's no reason for them to have access to it. For example,

in **BLU**, the FTC alleged the company didn't impose limits on the consumer information that one of its contractors could access. The contractor collected and transferred to its servers far more information than it needed to do its job, including the full content of consumers' text messages, real time location data, call and text message logs with full telephone numbers, and contact lists. The company could have protected this sensitive consumer data by implementing appropriate security procedures to oversee the security practices of its service providers, as well as by ensuring that only authorized employees or contractors with a legitimate business need had access to users' personal information.

The FTC's complaint in **MoviePass** alleged the company failed to protect its users' personal and financial information, including by storing this information in plain text and then by failing to impose restrictions on who could access the data. MoviePass stored consumer information, including names, email addresses, birth dates, credit card numbers, and geolocation information. The company then loaded the information onto a server on which it had disabled the firewall, leaving the data accessible to anyone with an internet connection. The resulting data breach could have been avoided by encrypting consumer data and by maintaining and managing security controls to protect and restrict access to that data.

Limit administrative access.

Administrative access, which lets a user make system-wide changes to your system, should be limited to the employees tasked with that job. In its action against **Uber**, for example, the FTC alleged the company failed to restrict access to systems based on employees' job functions, and allowed all programs and engineers to use a single Amazon Web Services (AWS) access key that gave full administrative privileges over all the company's data in the cloud storage service. As a result of this practice, when an engineer posted the key to a software development site, a malicious actor was able to use it to access the sensitive personal information of thousands of Uber drivers, including names and driver's license, bank account, and Social Security numbers.

3   Require secure passwords and authentication.

If you have personal information stored on your network, strong authentication procedures – including sensible password management – can help ensure that only authorized individuals can access the data. When developing your company's policies, here are lessons 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. Give some thought to the password standards you implement. In the FTC's 2011 *Twitter* case, for example, the FTC alleged that 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.

In *Drizly*, the FTC alleged the company failed to require unique and complex passwords or multifactor authentication for accessing the company's GitHub repositories. A Drizly executive reused a password he had used for other personal accounts, but his recycled password was exposed in an unrelated breach. This created an opportunity for a malicious actor to access Drizly's GitHub repositories, which made it possible for the attacker to access other database credentials and ultimately exfiltrate the personal information of 2.5 million consumers. The company could have reduced those risks by requiring that employees create unique and complex passwords (i.e., long passwords not used by the person for any other online service) or multifactor authentication to protect access to source code or databases. Even better, companies can require employees to use security keys for access.

Store passwords securely.

Don't make it easy for interlopers to access passwords. In the FTC's 2011 case against Twitter, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts. Twitter could have reduced the risk if it had policies and procedures in place to store credentials securely. Businesses should consider other protections to help protect against password compromises – for example, multi-factor authentication or strong adaptive and salted hashing that has significant iterations of the hashing algorithm for each password. In *Chegg*, the company allegedly shared its AWS root credentials among its employees and outside contractors, and didn't terminate or update those credentials when a contractor left. Later on, the former contractor was able to use the credentials to exfiltrate the personal information of 40 million Chegg users. Chegg could have protected its AWS root credentials by requiring that employees and contractors use distinct access keys, and requiring multifactor authentication for access to the company's AWS databases. Companies can also regularly rotate existing keys.

Guard against brute force attacks.

Remember that adage about an infinite number of monkeys at an infinite number of typewriters? Hackers use automated programs that perform a similar function. These brute force attacks work by typing endless combinations of characters until hackers luck into someone's password. Or hackers can try using stolen credentials from other data breaches. In the *TaxSlayer* case, the FTC alleged the company failed to implement adequate risk-based authentication measures. As a result, malicious hackers were able to gain full access to nearly 9,000 consumer accounts, and then used the stolen information to commit tax identity theft.

According to the FTC, TaxSlayer failed to put a number of protective measures in place to reduce the risk to consumers' sensitive information. For example, TaxSlayer could have taken steps to neutralize list validation attacks, used readily-available tools to prevent devices or IP addresses from attempting to access an unlimited number of accounts in rapid succession, and conducted a risk assessment that would have identified reasonably foreseeable threats associated with inadequate authentication. Companies can also prevent users from using passwords that are known to have been compromised in previous breaches.

Protect against authentication bypass.

Locking the front door doesn't offer much protection if the back door is open. In *Lookout Services*, the FTC charged that the company failed to adequately test its web application for widely known security flaws, including one called "predictable resource location." As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app's authentication screen and gain unauthorized access to the company's databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.

---

4   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 include Transport Layer Security (TLS) 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 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 offices. That risk could have been prevented by ensuring the data was secure throughout its lifecycle, 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 effective standards that can apply to your business. Don't start from scratch when it isn't necessary. Instead, take advantage of collected wisdom. The *Lenovo* case illustrates that principle. According to the FTC, the company used an insecure method to replace digital certificates on encrypted websites with certificates signed by its own software. However, its software didn't adequately verify that the websites' digital certificates were valid before replacing them. The company could have avoided this weakness by using tried-and-true industry-tested and accepted methods for authenticating websites.

Ensure proper configuration.

Even the strongest encryption 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 the companies used SSL encryption in their mobile apps, but turned off 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.

<table>
<tr><td>**5**</td><td></td></tr>
</table>

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

When designing your network, consider using tools to validate and limit implicit trust between networked systems. Assume that all traffic regardless of source is hostile. Part of your "zero trust" toolkit should be tools to inspect and log network traffic — like SIEM and SOAR tools to monitor your network for malicious activity. Here are some lessons from FTC cases to consider when designing your network.

Continuously validate access to data.

Not every computer in your system needs to be able to communicate with every other one. Help protect particularly sensitive data by housing it in a separate secure place

on your network. That's a lesson from the *Infotrax* case. The FTC alleged the company didn't sufficiently limit one client's distributors from accessing another client's data on the network. As a result, hackers penetrated the company's server through a single client's website and could then access every client's consumer data on the network.
The company could have reduced that risk by continuously validating access to its data.

Monitor activity on your network.

"What's happening on my network?" An effective SIEM tool will allow your security staff to answer that question.

In *i-Dressup*, the FTC alleged that the company didn't use an intrusion detection and prevention system. After a hacker accessed the company's computer network and compromised the personal information of about 245,000 children under the age of 13, the company learned of the breach only after hearing from a journalist who had been in contact with the hacker. The company could have detected this data breach much earlier by using readily available and low-cost security measures to alert them to instances of unauthorized access to their network.

More generally, in the *DealerBuilt* case, the FTC alleged the company didn't use security measures to monitor its systems and assets. As a result, when an employee connected a storage device to the company's backup network without ensuring it was securely configured, the resulting insecure connection created an opportunity for a hacker to breach the backup database. The FTC said that hacker then downloaded the personal information of tens of thousands of consumers, including their Social Security and driver's license numbers, birth dates, and financial information. The company could have identified this breach sooner by using readily available tools to monitor its systems.

Security-centric companies may consider using "canaries" to help uncover unauthorized access attempts. What's a canary? It's a ruse designed to test if intruders are trying to get into your system without actually putting your network at risk. This could involve, for example, adding hardware or software to a mock network that doesn't really interact with your system. If something does try to interact with it, that's a sign you may have an intruder moving around your network.

6 ▸ Secure remote access to your network.

Business doesn't just happen in the office. 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 example, in *Premier Capital Lending*, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business's security. When hackers accessed the client's system, they stole its remote login credentials and used them to grab consumers' personal information. According to the complaint in *Settlement One*, the business allowed clients that didn't have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal.

And in LifeLock, the FTC charged that the company failed to install antivirus programs on the computers that employees used to access its network remotely. Businesses today could reduce these risks by using endpoint detection and response, as well as extended detection and response security solutions – often called EDR/XDR tools – to strengthen security of network endpoints and allow faster detection and response to security incidents.

Put sensible access limits in place.

Not everyone who might occasionally need to get on your network should have an all-access, backstage pass. Instead, limit access based on the parameters of a particular task. In the *Dave & Buster's* case, for example, the FTC charged that the company failed to adequately restrict third-party access to its network. By exploiting security weaknesses in the third-party company's system, an intruder allegedly connected to Dave & Buster's network numerous times and intercepted personal information. What could Dave & Buster's have done to reduce that risk? It could have placed limits on third-party access

to its network – for example, by closely monitoring connections to sensitive data or by granting temporary access carefully restricted to what the third party needed to get the job done.

7 ▶ Apply sound security practices when developing new products.

So you have a great new app or innovative software on the drawing board. Early in the development process, think through how customers will likely use the product. If they'll be storing or sending sensitive information, is your product up to the task of handling that data securely? Before going to market, consider the lessons from FTC cases involving product development, design, testing, and roll-out.

Train your engineers in secure coding.

Have you explained to your developers the need to keep security at the forefront? In cases like *Tapplock* and *Zoom*, the FTC alleged the companies failed to train their employees in secure coding practices. In Tapplock, the FTC said the company touted the security of its locks, including their digital security. The company's smart locks collected consumers' personal information, including usernames, email addresses, profile photos, and the locks' precise locations. However, according to the FTC, the locks were subject to vulnerabilities that prevented consumers from effectively revoking access to their locks. Security researchers found they could bypass Tapplock's account authentication process and access user data. The company could have avoided these issues by implementing a security program that included vulnerability and penetration testing of its locks, ensuring that effective safeguards were in place to protect consumer data, and training its software engineers in secure coding practices.

In Zoom, the FTC alleged the company compromised some users' security when it secretly installed software, called a ZoomOpener web server, as part of a manual update for its Mac desktop application. When operating as usual, before launching the Zoom app, Apple's Safari browser would display a warning box that asked users if they wanted to launch the app. But the ZoomOpener web server allowed Zoom to automatically launch and join a user to a meeting – thereby bypassing the Safari safeguard that protected users from a common type of malware. According to the complaint, Zoom's

covert installation of ZoomOpener increased the risk of remote video surveillance by strangers, and the company didn't implement any offsetting measures to protect users' security. What's more, the software remained on users' computers even after they deleted the Zoom app, and in certain circumstances would even reinstall the app automatically without any action by the user. The company could have avoided this vulnerability by implementing a training program on secure software development practices.

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 the companies failed to follow explicit platform guidelines about secure development practices. For example, the FTC alleged that Fandango and Credit Karma turned off a critical process known as 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 off certificate validation. The advice for other companies: When choosing among third-party tools and platforms, pick ones that are designed for security, and have safe defaults that mitigate risks out of the box.

Verify that privacy and security features work.

If your software offers 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 recover the video files with common file browsing tools. The lesson for other companies: When offering privacy and security features, ensure that your product lives up to your advertising claims.

Test for common vulnerabilities.

There is no way to anticipate every threat, but some vulnerabilities are commonly known and reasonably foreseeable. In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in **D-Link**, the FTC alleged the company failed to perform basic procedures essential to secure software development, including testing and remediation to address well-known and preventable security flaws. As a result, D-Link's routers and internet-connected cameras were left exposed to third parties and vulnerable to hackers.

Similarly, in **CafePress**, the FTC alleged the company failed to protect its website against the common Structured Query Language (SQL) injection attack, resulting in the exposure of sensitive consumer information like Social Security numbers. That's a risk that could have been avoided if CafePress had tested for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).

8 ▸ 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 develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In **GMR Transcription**, for example, the FTC alleged the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed online. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can't be a "take our word for it" thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process. The *Upromise* case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to "remove any personally identifiable information" before transmission.

But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted it in clear text. How could Upromise have reduced that risk? By asking questions and following up with the service provider during the development process.

9 ▸ 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 the company didn't update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business's defenses. Similarly in *Equifax*, the FTC alleged the company failed to patch a critical vulnerability, in part

because its patch management policies and procedures were inadequate. Depending on the complexity of your network or software, you may need to prioritize patches by the severity of the threat they are designed to avert. Nonetheless, having a reasonable process in place to update and patch third-party software is an important step toward reducing the risk of a compromise. Consider using automated tools to track which versions of software your system is running and whether updates are available.

Heed credible security warnings and move quickly to fix them.

When vulnerabilities come to your attention, listen carefully and then get a move on. In the HTC America case, the FTC charged that the company didn't have a process for receiving and addressing reports about security vulnerabilities. HTC's alleged delay in responding to warnings meant that the vulnerabilities found their way onto even more devices across multiple operating system versions.

Sometimes companies receive security alerts, but they get lost in the shuffle. In Fandango, for example, the company relied on its general customer service system to respond to warnings about security risks. According to the complaint, when a researcher contacted the business about a vulnerability, the system incorrectly categorized the report as a password reset request, sent an automated response, and marked the message as "resolved" without flagging it for further review. As a result, Fandango didn't learn about the vulnerability until FTC staff contacted the company. The lesson for other businesses? Have an effective process in place to receive and address security vulnerability reports. Consider a clearly publicized and effective channel (for example, a dedicated email address like security@yourcompany.com) for receiving reports and flagging them for your security staff.

10 ▸ Secure paper, physical media, and devices.

Network security is a critical consideration, but many of the same lessons apply to paperwork and physical media like hard drives, laptops, flash drives, and disks. FTC cases offer some things to consider when evaluating physical security at your business.

Securely store sensitive files.

If it's necessary to retain important paperwork, take steps to keep it secure. In the *Gregory Navone* case, the FTC alleged the defendant maintained sensitive consumer information, collected by his former businesses, in boxes in his garage. In *LifeLock*, the complaint charged that the company left faxed documents that included consumers' personal information in an open and easily accessible area. In each case, the business could have reduced the risk to their customers by implementing policies to store documents securely.

Protect devices that process personal information.

Securing information stored on your network won't protect your customers if the data has already been stolen through the device that collects it. In the *Dollar Tree* investigation, FTC staff said that the business's PIN entry devices were vulnerable to tampering and theft. As a result, unauthorized persons could capture consumers' payment card information, including the magnetic stripe data and PIN, through an attack known as "PED skimming." Given the novelty of this type of attack at the time, and a number of other factors, staff closed the investigation. However, attacks targeting point-of-sale devices are now common and well-known, and businesses should take reasonable steps to protect such devices from compromise.

Keep safety standards in place when data is en route.

Understand the importance of securing sensitive information when it's outside the office. In Accretive, for example, the FTC alleged an employee left a laptop containing more than 600 files, with 20 million pieces of information related to 23,000 patients, in the locked passenger compartment of a car, which was then stolen. The *CBR Systems* case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive — all of which contained sensitive information — that were lifted from an employee's car. In each case, the business could have reduced the risk to consumers' personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets you track where the package is. Limit the instances when employees need to be out and about with sensitive data in their possession. But when there's a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.

Dispose of sensitive data securely.

Paperwork or equipment you no longer need may look like trash, but it's treasure to identity thieves if it includes personal information about consumers or employees. For example, according to the FTC complaints in *Rite Aid* and *CVS Caremark*, the companies tossed sensitive personal information – like prescriptions – in dumpsters In *Goal Financial*, the FTC alleged an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text. The companies could have prevented the risk to consumers' personal information by shredding, burning, or pulverizing documents to make them unreadable and by using available technology to wipe devices that aren't in use.

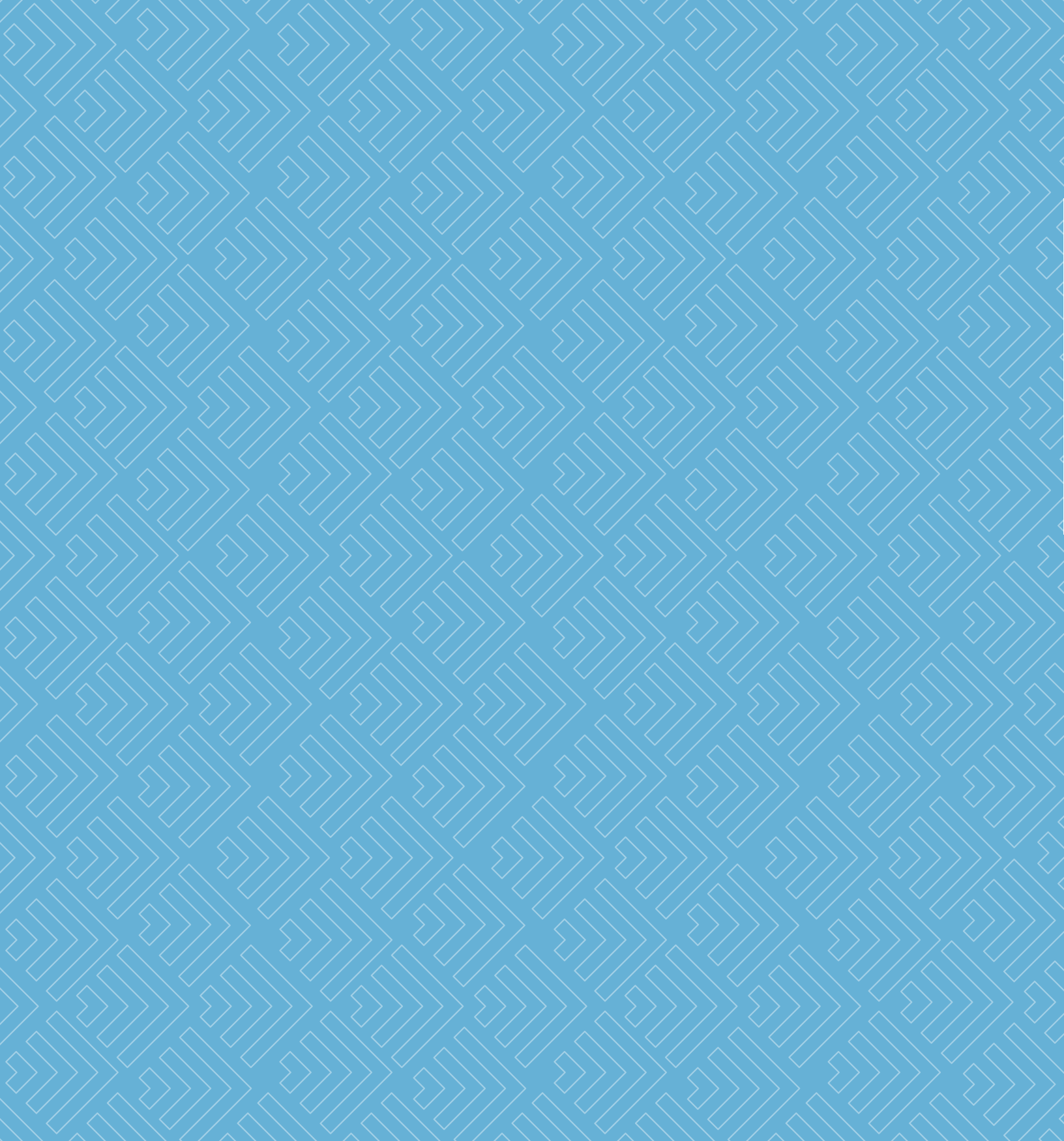## Looking for more information?

Visit the Data Security section of **business.ftc.gov** for a listing of relevant cases and other free resources.

About the FTC

The FTC works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers. Report scams and bad business practices at **ReportFraud.ftc.gov**. We also provide guidance at **business.ftc.gov** to help companies comply with the law. Regardless of the size of your organization or the industry you're in, knowing — and fulfilling — your compliance responsibilities is smart, sound business. Looking for a quick take on recent cases and other initiatives? Subscribe to the **FTC's Business Blog**.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman**.