Protecting PERSONAL INFORMATION

A Guide for Business

FEDERAL TRADE COMMISSION

PROTECTING PERSONAL INFORMATION

A Guide for Business

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

Some businesses may have the expertise in-house to implement an appropriate plan. Others may find it helpful to hire a contractor. Regardless of the size—or nature—of your business, the principles in this brochure will go a long way toward helping you keep data secure.

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)
business.ftc.gov/privacy-and-security

A sound data security plan is built on **5 key principles:**

1. **Take stock.** Know what personal information you have in your files and on your computers.

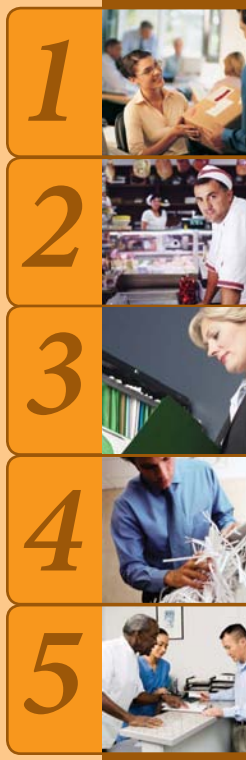
2. **Scale down.** Keep only what you need for your business.

3. **Lock it.** Protect the information that you keep.

4. **Pitch it.** Properly dispose of what you no longer need.

5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary. You also can take an interactive tutorial at ***business.ftc.gov/privacy-and-security***.



1. TAKE STOCK. Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, digital copiers, and mobile devices? No inventory is complete until you check everywhere sensitive data might be stored.
- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:
  - ***Who sends sensitive personal information to your business.*** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Job applicants? Other businesses?
  - ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
  - ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
  - ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On employees' smartphones, tablets, or other mobile devices? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?
  - ***Who has—or could have—access to the information.*** Which of your employees has permission to access the information? Do they need access? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?
- Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

SECURITY CHECK

Question:
Are there laws that require my company to keep sensitive data secure?

Answer:
Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit ***business.ftc.gov/privacy-and-security***.

2. SCALE DOWN. Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

SECURITY CHECK

Question:

We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collect from the magnetic stripe on their credit cards. Could this put their information at risk?

Answer:

Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers.

- The law requires you to shorten—or truncate—the electronically printed credit and debit card receipts you give your customers. You may include no more than the last five digits of the card number, and you must delete the expiration date.
- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Check the default settings on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not keeping information you don't need.
- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

3. LOCK IT. Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.
- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.
- If you have devices that collect sensitive information, like PIN pads, secure them so that identity thieves can't tamper with them. Also inventory those items to ensure that they have not been switched.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

General Network Security

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- Check expert websites (such as ***www.sans.org***) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Consider restricting employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

SECURITY CHECK

Question:

We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the Internet to our branch offices in regular text. Is there a safer practice?

Answer:

Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or identity thieves.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

Password Management

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different, and require frequent changes in passwords.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.
- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.

SECURITY CHECK

Question:

Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

Answer:

Yes. Hackers will first try words like "password," your company name, the software's default password, and other easy-to-guess choices. They'll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. And change passwords often.

- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.
- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.
- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.

- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

Firewalls

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you should install a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

- Determine if you use wireless devices like smartphones, tablets, or inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.
- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.
- Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Digital Copiers

Your information security plan should cover the digital copiers your company uses. The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes, or emails. If you don't take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extraction once the drive has been removed.

Here are some tips about safeguards for sensitive data stored on the hard drives of digital copiers:

- Get your IT staff involved when you're thinking about getting a copier. Employees responsible for securing your computers also should be responsible for securing data on digital copiers.
- When you're buying or leasing a copier, consider data security features offered, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting. Encryption scrambles the data on the hard drive so it can be read only by particular software. Overwriting—also known as file wiping or shredding—replaces the existing data with random characters, making it harder for someone to reconstruct a file.
- Once you choose a copier, take advantage of all its security features. You may be able to set the number of times data is overwritten—generally, the more times the data is overwritten, the safer it is from being retrieved. In addition, make it an office practice to securely overwrite the entire hard drive at least once a month.

- When you return or dispose of a copier, find out whether you can have the hard drive removed and destroyed, or overwrite the data on the hard drive. Have a skilled technician remove the hard drive to avoid the risk of breaking the machine.

To find out more, read *Copier Data Security: A Guide for Businesses*.

Detecting Breaches

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.
- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See pages 22–23 for more information.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.

SECURITY CHECK

Question:

I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

Answer:

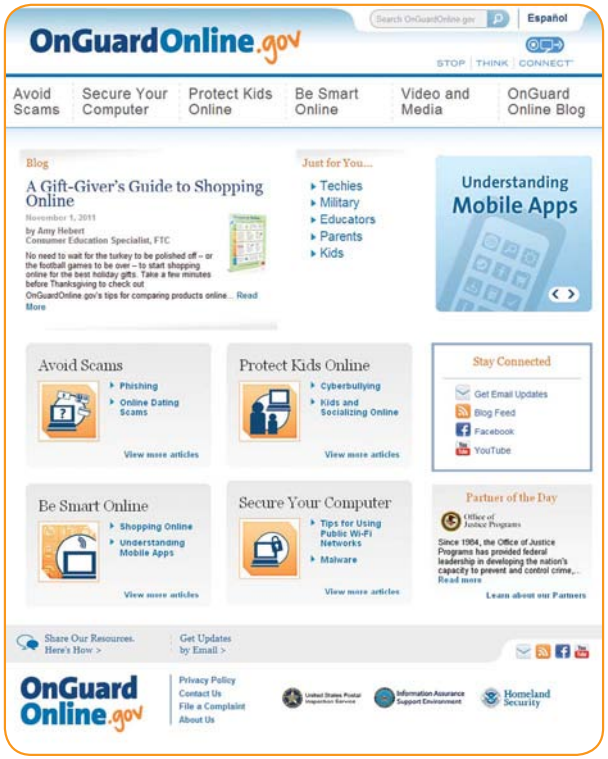
Yes. There are simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system. Protect your systems by keeping software updated and conducting periodic sercurity reviews for your network. Bookmark the websites of groups like the Open Web Application Security Project, ***www.owasp.org***, or SANS (SysAdmin, Audit, Network, Security) Institute's The Top Cyber Security Risks, ***www.sans.org/top-cyber-security-risks***, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.
- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

- Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

Consider asking your employees to take the FTC's plain-language, interactive tutorial at ***business.ftc.gov/privacy-and-security***.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information. When verifying, do not reply to the email and do not use links, phone numbers, or websites contained in the email.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.



SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Address security issues for the type of data your service providers handle in your contract with them.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. PITCH IT. Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

SECURITY CHECK

Question:

My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

Answer:

No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

- Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.
- When disposing of old computers and portable storage devices, use software for securely erasing data, usually called wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.
- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.
- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How*.

5. PLAN AHEAD. Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.

SECURITY CHECK

Question:

I own a small business. Aren't these precautions going to cost me a mint to implement?

Answer:

No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

- If a computer is compromised, disconnect it immediately from your network.
- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- **National Institute of Standards and Technology (NIST)**
  Computer Security Resource Center
  www.csrc.nist.gov

- **SANS (SysAdmin, Audit, Network, Security) Institute**
  The Top Cyber Security Risks
  www.sans.org/top-cyber-security-risks

- **United States Computer Emergency Readiness Team (US-CERT)**
  www.us-cert.gov

- **OnGuard Online**
  www.OnGuardOnline.gov

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit ***ftc.gov*** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.

Watch a video, *How to File a Complaint*, at ***ftc.gov/video*** to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

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 ***www.sba.gov/ombudsman***.

November 2011

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)
business.ftc.gov/privacy-and-security

Consumer Problem Got You Down?

We'll Stand Up For You!

Office of Consumer Protection

Ensuring Integrity in the Marketplace

- Complaint Investigation & Conciliation
- Education
- Law Enforcement
- Pre-Purchase Information
- Mediation
- Legislative Advocacy
- Common Ownership Communities
- Services Available in Spanish

100 Maryland Avenue
Suite 330 / Rockville, MD 20850

www.montgomerycountymd.gov/consumer

Anonymous Consumer Tip Line:
(240) 777-3681

240-777-3636