Control the Risk of Identity Theft

Guidance for Your Business

NORTH AMERICAN EQUIPMENT DEALERS ASSOCIATION

This information was compiled from
Protecting Personal Information: A Guide for Business,
a publication of the Federal Trade Commission.

Control the Risk of Identity Theft

Guidance for Your Business

Introduction

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) became law on December 4, 2003. FACTA added several new provisions to the Fair Credit Reporting Act of 1970 and directs numerous federal agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft.

The Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); the Federal Deposit Insurance Corporation (FDIC); the Office of Thrift Supervision, Treasury (OTS); the National Credit Union Administration (NCUA); and the Federal Trade Commission (FTC) issued joint final rules and guidelines that went into effect January 1, 2008. **Mandatory compliance for businesses, including equipment dealerships, of these rules starts on November 1, 2008.**

What the law and rules mean to dealers

It is almost impossible to be in business and not collect or hold personal information – names and addresses, Social Security numbers, credit card numbers, or other account numbers – about your customers, employees and business partners. If this information falls into the wrong hands, it could put those individuals at risk for identity theft and make you and your dealership legally liable for any adverse consequences from the theft of personal information.

Not all personal information compromises result in identity theft, and the type of personal information compromised can significantly affect the degree of potential damage. The steps a dealership should take and whom a dealership should contact if personal information is compromised is spelled out in this document.

Steps dealers need to take

A sound dealership security plan for personal information is mandated by the new regulations and consists of 5 key principles:

1. **Take stock.** Know what personal information your dealership has in its files and on its computers.
2. **Scale down.** Keep only the information your dealership needs for business.
3. **Lock it.** Protect the information your dealership keeps.
4. **Pitch it.** Properly dispose of what your dealership no longer needs.
5. **Plan ahead.** Have a written plan approved by senior management or board of directors in place for the above items, train dealership staff on how to handle personal information and include in the written plan how your dealership will respond to security breech incidents.

A check list for dealerships to use and make changes where necessary follows.

1. Take stock.

Know what personal information your dealership has in its files and on its computers.

Effective data security begins with assessing what information your dealership has and identifying who has access to it. Understanding how personal information moves into, through, and out of your dealership and who has – or could have – access to it is essential to assessing security vulnerabilities. Dealer principals can best determine the ways to secure the information only after they have determined how it flows.

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment to find out where your dealership stores sensitive data. Also, inventory the information your dealership has by type and location. File cabinets and computer systems are a start, but remember that most dealerships receive personal information in a number of ways – through Web sites, from contractors, from call centers, faxes, sales orders, credit cards, employee or finance applications, etc. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until your dealership has checked everywhere sensitive data might be stored.
- Track personal information in your dealership by talking with the sales department, information technology (IT) staff, human resources office, accounting personnel, and outside service providers. It's important to completely understand the following:
  Who sends sensitive personal information to your dealership. Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?
  How your dealership receives personal information. Does it come to your dealership through a Web site? By e-mail? Postal delivery? Is it transmitted through cash registers or electronic business systems?
  What kind of information your dealership collects at each entry point. Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
  Where your dealership keeps the information collected at each entry point. Is it in a central computer database? On individual laptops used inside and outside your dealership? 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 dealership's employees have permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software your dealership used for customer account information or to process credit card transactions?
- Different types of information present varying risks. Pay particular attention to how your dealership keeps personal information: Social Security numbers, credit card or financial information, and other sensitive data. This is what thieves most often use to commit fraud or identity theft.

2. Scale down.

Keep only the information your dealership needs for the business.

If your dealership doesn't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If your dealership has 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, such as 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.
- Don't keep a customer's credit card information unless there is a business need for it. For example, don't retain the account number and expiration date. Keeping this information – or keeping it longer than necessary – raises the risk the information could be used to commit fraud or identity theft.
- Check the default settings on your dealership's 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 it's not inadvertently keeping information not needed.
- If your dealership 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 it is no longer needed.

3. Lock it.

Protect the information your dealership keeps.

What's the best way to protect the sensitive personal information your dealership needs to keep? It depends on the kind of information and how it's stored. The most effective data security plan deals 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, CDs, floppy disks, zip drives, tapes, and backups containing personal information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need and control who has a key, and the number of keys issued.
- Require that files containing personal 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.
- Put appropriate access controls into place for dealership buildings. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If your dealership maintains offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If your dealership ships 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 your dealership to track the delivery of the information.

Electronic Security

Computer security isn't just the realm of a dealership's IT staff. Make it the dealership's business to understand the vulnerabilities of its 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 sensitive information is stored. This may include the Internet, electronic cash registers, computers at branch offices, computers used by service providers to support your dealership's network, wireless devices, such as inventory scanners or cell phones.
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your dealership's 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 your dealership sends to third parties over public networks, i.e., the Internet. Consider encrypting sensitive information that is stored on dealership computer networks or on disks or portable storage devices used by employees. Consider also encrypting e-mail 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 dealership's network.
- Check your dealership's software vendors' Web sites regularly for alerts about new vulnerabilities, and put policies into place for installing vendor-approved patches to correct problems.
- Scan computers on dealership networks to identify and profile the operating system and open network services. If services are found that your dealership doesn't need, disable them to prevent hacks or other potential security problems. For example, if e-mail service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on the computer to prevent unauthorized access to the 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.

- Pay particular attention to the security of Web applications – the software used to give information to visitors to your dealership's Web site and to retrieve information from it. 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 dealership's 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 employees to use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords, such as 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 dealership policy to share their passwords or display 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 a dealership's staff or a customer. Let employees know that such calls are always fraudulent, and that no one should be asking them to reveal their passwords.
- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personal information and data – Social Security numbers, passwords, or account information – via e-mail. Unencrypted e-mail is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to 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 store the information on their laptops. Using this approach, the information is stored on a secure central computer and the laptops function as terminals that display (but don't store) information from the central computer. 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 any data on a computer that is reported stolen will be destroyed when a thief uses it to try to get on the Internet.

- Train employees to be mindful of security when they're traveling. 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 through the screening process.

Firewalls

- Use a firewall to protect your dealership's computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing a computer. A properly configured firewall makes it tougher for hackers to locate a dealership's computer and get into its programs and files.
- Determine whether your dealership should install a "border" firewall where the 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 a dealership's sensitive information is stored. 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, a dealership should review them periodically.
- If some computers on a dealership's 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 your dealership uses wireless devices like inventory scanners or cell phones to connect to its computer network or to transmit sensitive information.
- If your dealership does use wireless or remote access, consider limiting who can use a wireless connection to access the computer network. By limiting the wireless devices that can connect to your network, your dealership can make it more difficult for an intruder to access the network.
- Even better, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your dealership's computer network may prevent an intruder from gaining access through a process called "spoofing" – impersonating one of your computers to get access to your dealership's network.
- Consider using encryption if your dealership allows remote access to its computer network by employees or by service providers, such as companies that troubleshoot and update software, particularly if your dealership uses them to process credit card purchases.

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 dealership's network so management can spot and respond to attacks. If there is an attack on a dealership's 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 the dealership 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.

Employee Training

Your dealership's data security plan may look great on paper, but it's only as strong as the employees who put it into place. Take time to explain the rules to your dealership's staff and train them to spot security vulnerabilities. Periodic training emphasizes the importance the dealership places 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.
- Ask every new employee to sign an agreement to follow your dealership's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your dealership's data security plan is an essential part of their duties. Regularly remind employees of your dealership'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 employees who leave the dealership or transfer to another part of the dealership 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 creating 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 openly reward employees who alert you to vulnerabilities.
- Tell employees about your dealership's 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 the dealership's policies cover employees who telecommute or access sensitive data from home or an offsite location.
- 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 requesting company using a phone number known to be genuine.
- Require employees to notify the dealership immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.

Security practices of contractors and service providers

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

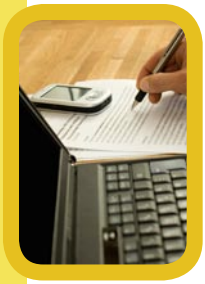
- Before your dealership outsources any of its business functions – payroll, Web hosting, customer call center operations, data processing, etc. – investigate that company's data security practices and compare their standards to that of the dealerships. If possible, visit their facilities.
- Address security issues for the type of data your dealership's service providers handle in the 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 your dealership no longer needs.

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

- Establish information disposal practices that are reasonable and appropriate to prevent unauthorized access to – or use of – personal information. Reasonable measures for your dealership should be based on the sensitivity of the information, the costs and benefits of different disposal methods and changes in technology.
- 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 programs that wipe (or clean) data drives. Deleting files using keyboard or mouse commands generally aren'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.



5. Plan ahead.

Have a written plan (that includes items 1 through 4) approved by senior management or board of directors; train dealership staff on how to handle personal information; and include in the plan how your dealership will respond to security breech incidents.

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

- Have a plan in place to respond to security incidents. Designate a senior member of your dealership's staff to coordinate and apply the response plan.
- If a computer is compromised, disconnect it immediately from the Internet.
- 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. Dealerships 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.

What to do if your dealership has an identity theft

Notifying Law Enforcement

When the compromise could result in harm to a person or business, call your local police department immediately. Report your dealership's situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective it can be. If local authorities are not familiar with investigating information compromises, contact a local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service. Check the blue pages of your telephone directory or conduct an online search engine for the number of the nearest federal field offices.

Notifying Affected Businesses

Information compromises can have an impact on businesses other than the dealership's, such as banks or credit issuers. If account access information – e.g., credit card or bank account numbers – has been stolen from a dealership, but the dealership does not maintain the accounts, notify the institution that does so it can monitor the accounts for fraudulent activity. If a dealership collects or stores personal information on behalf of other businesses, notify them of any information compromise.

If names and Social Security numbers have been stolen, the dealership can contact the major credit bureaus for additional information or advice. If the compromise involves a large group of people, advise the credit bureaus if the dealership is recommending that people request fraud alerts for their files. Your notice to the credit bureaus can facilitate customer assistance. Those contact numbers are:

Equifax: 1-800-685-1111
Experian: 1-888-397-3742
TransUnion: 1-800-372-8391

If the information compromise resulted from the improper posting of personal information on a dealership's Web site, immediately remove the information from the site. Be aware that Internet search engines store, or "cache," information for a period of time. A dealership can contact the search engines to ensure that they do not archive personal information that was posted in error.

Notifying Individuals

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Social Security numbers can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take some steps to prevent or limit any harm.

When notifying individuals, the FTC recommends that your dealership: • consult with the local law enforcement contact about the timing of the notification so it does not impede the investigation.• designate a contact person within your dealership for releasing information. Give the contact person the latest information about the breach, your dealership's response, and how individuals should respond. Consider using letters (see examples herein), Web sites, and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your dealership's notice;

- describe clearly what your dealership knew about the compromise. Include how it happened, what information was taken and, if known, how thieves have used the information, and what actions your dealership has taken to remedy the situation. Explain how to reach the contact person in your dealership.
- explain what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports.
- include current information about identity theft. The FTC's Web site at **www.ftc.gov/idtheft** has information to help individuals guard against and deal with identity theft.
- provide contact information for the law enforcement officer working on the case (as well as the case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working the case that your dealership is sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.

- encourage those who discover that their information has been misused to file a complaint with the FTC at **www.ftc.gov/idtheft** or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

Model Letter

The letter attached is a model for notifying people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

This letter may be copied to a Word document by using the Text Select Tool located on the toolbar in this .pdf file.

Model Letter

for the compromise of social security numbers and personal information

Dear_____:

We are contacting you about a potential problem involving identity theft.
[Describe the information compromise and how your dealership is responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

- Equifax: 888-397-3742
- Experian : 888-397-3742
- TransUnion: 800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts.

You also should file a complaint with the FTC at **www.ftc.gov/idtheft** or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for its investigations.

[Insert closing]

Dealership / Principal Name

DRAFT

This letter may be copied to a Word document by using the Text Select Tool located on the toolbar in this .pdf file.

FACTA

Compliance Plan for [Your Dealership's Name]

This Plan is designed to bring this dealership into compliance with FACTA and will be reviewed on an annual basis or as needed.

I. Assessment of Information Collected and Stored at the Dealership

1. Inventory all computers, laptops, flash drives, disks, home computers, cell phones and other equipment where sensitive data is stored.
2. Inventory sensitive data stored in file cabinets, desks and files in sales, human resource, accounting, parts and service offices.
3. Person(s) responsible for assessments under this section is _____ .

II. Records Destruction

1. Destroy all records deemed unnecessary from the assessment in Section I of this document.
2. Person(s) responsible for destruction of documents is _____ .

III. Protection of Information

1. Secure information that is maintained by locking files, office doors and ensuring that computer and server information is also secured.
2. Person(s) responsible for the protection of documents is _____ .

IV. Employee Training

1. Assign an employee who is responsible for employee training on how important it is that employees secure critical information and notify management of data security vulnerabilities.
2. Training will include: how to recognize security threats, how to report suspicious activity, company policies on sensitive data security, possible phone phishing scams and company discipline measures for security policy violations.

(continued)

3. Person(s) responsible for employee training is _____ .

V. Dealership Action Plan for a Breach of Security

1. Notifying Law Enforcement – When a data compromise is found and determined it could result in harm to a person or business, the local police department will be notified. The dealership will report the situation and the potential risk for identity theft. If the local police request, additional contacts will be made to the local office of the FBI, U.S. Secret Service or the U.S. Postal Inspection Service.
2. Notifying Affected Businesses and Individuals – If account access information has been stolen from your dealership, the dealership will notify the business or individual that their information has been stolen. The dealership may also contact the major credit bureaus and report the theft or offer sources for additional information or advice. If the compromise involves a large group of people, the credit bureaus will be advised that the dealership is recommending that people request fraud alerts for their files. The contact numbers that will be used are:
   - Equifax: 800-685-1111
   - Experian: 888-397-3742
   - TransUnion: 800-372-8391
3. The Model Letter associated with this plan will be sent, as needed, to inform businesses and individuals of stolen identify information.

This Plan was adopted by [senior management and/or board of directors] on [date].