PROTECT YOUR BUSINESS FROM ID THEFT

Guard Your Clients' Information
Identity thieves target businesses from large companies to small stores. They're seeking your customers' and employees' personal information. Here are some tips to help your business keep this information safe.

Collection of Personal Information
Avoid asking customers for private information, unless no other option is available. When you must ask for personal information, avoid doing it in front of other customers or where it could be seen or overheard.

Stop using Social Security numbers or driver's license numbers as account numbers.

Don't collect Social Security numbers on job applications until selecting the applicant. Once you've selected a new employee, consider conducting criminal and civil background checks, particularly if the employee will have access to sensitive information.

Pick passwords and usernames that don't include personal information. Turn computer screens away from public view.

Protect Personal Information
Limit customers and vendors to designated public areas. Limit access to documents and files that contain personal information to key managers who need it.

When an employee leaves, immediately remove their access to computer networks and confidential files. Verify third party requests for personal information to make sure they have a legitimate purpose for getting the information.

Put security procedures in place for documents that contain personal identifying information. Keep documents with personal information in locked file cabinets. At a minimum, make sure that all vital records and offices are locked during non-business hours. Regularly brief employees and management about security policies, security threats and how to report a problem.

Protect Computers
Set a laptop security policy. Limit access to computers by using passwords or multi-factor authentication. Put additional security measures in place, such as firewalls, anti-virus software, spyware protection software and encryption software.

Use data protection software to record network activity and regularly check logging data and audit trails for suspicious activity. Avoid file sharing or making files containing personal information available through a network or the Internet, unless it's absolutely necessary.

Protect Correspondence
Keep incoming mail in a locked mailbox. Don't mail, email or fax bills or other correspondence to customers that include personal information. Include only part of the employee or customer's SSN if it's necessary to include it at all.

Dispose of Personal Information
To reduce the harm to customers and staff if your records fall into the wrong hands, get rid of records you don't need anymore. At a minimum, old documents containing personal information should be destroyed using a cross-cut paper shredder.

When you get a new computer, make your old computer hard-drive unreadable. After you back up your data and transfer the files elsewhere, sanitize the hard disk by shredding it, magnetically cleaning it or using software to wipe the disk clean. Make sure there isn't additional hardware related to the company's local area network. Destroy old computer disks and backup tapes.

Identity Theft Protection Act
The Identity Theft Protection Act requires businesses to take steps to protect their customers' personal information.

To protect your customers, your business must:

- Not include an individual's SSN on written correspondence to the individual unless it is required by state or federal law.
- Shred or destroy documents you dispose of that include customers' personal information.
- Notify your customers promptly if a security breach may have compromised their personal information and placed them at risk of identity theft.
- Notify the Consumer Protection Division of the NC Attorney General's Office. Failure to do so may result in penalties under N.C.G.S. § 75-15.2. Use our breach reporting form.
-

If you need legal advice about complying with the law, consult a private attorney