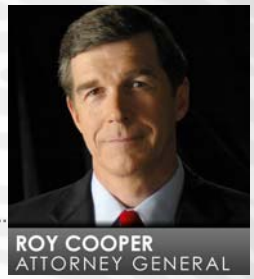
noscamnc.gov



Protect Your Business

Guard Your Clients' Information

Identity thieves are targeting businesses from large companies to small stores seeking to steal customers' and employees' personal information. Here are some tips to help your business keep this information out of the hands of identity thieves

COLLECTION OF PERSONAL INFORMATION

Avoid asking your customers for private information, unless no other option is available.

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

Don't collect SSNs on job applications until selecting the applicant. Once you've selected a prospective 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.

Avoid asking customers to provide you with necessary personal information in front of other customers or where the information could be seen or overheard.

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 identifying information to key managers who need to see it.

When an employee leaves, immediately remove their access to computer networks and confidential files.

Verify third party requests for personal information by contacting the requesting agency and taking reasonable steps to make sure they have a legitimate purpose for getting the information.

Implement security procedures for safeguarding documents that contain personal identifying information.

Keep documents containing personal information in locked file cabinets. At a minimum, ensure that all vital records and offices are locked during non-business hours.

Regularly brief employees and management about security policies, security threats, corrective measures and incident reporting procedures.

PROTECT COMPUTERS

Institute a laptop security policy.

Limit access to computers by using employee passwords.

Put additional security measures in place, such as firewalls, anti-virus software, spyware protection software, and encryption software.

Use data protection software that records network activity and regularly check logging data and audit trails for unusual or suspicious activity.

Avoid file sharing or access to files containing personal identifying information via a network or the Internet, unless it is absolutely necessary.

PROTECT CORRESPONDENCE

Keep incoming mail in a locked mailbox.

Don't mail, e-mail, or fax bills or other correspondence to customers that include personal identifying information.

Include only part of the employee or customer's SSN if it is necessary to include it at all.

DISPOSE OF PERSONAL INFORMATION

Shred or destroy documents and records containing personal identifying information when you dispose of them. At a minimum, employees should destroy old documents containing personal information using a cross-cut paper shredder.

Make old computers' hard-drives unreadable. After you back up your data and transfer the files elsewhere, you should sanitize by disk shredding, magnetically cleaning the disk, 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 Act of 2005

The Identity Theft Protection Act of 2005 places specific restrictions on the commercial use, maintenance, and destruction of Social Security Numbers (SSN). In addition, businesses must notify customers if they are at risk for identity theft due to a security breach. Under the Act, businesses must protect their customers by:

- Not including an individual's SSN on written correspondence to the individual unless it is required by state or federal law.
- Shredding or destroying documents they dispose of that include customers' personal information.
- Notifying their customers promptly if a security breach may have compromised their personal information and placed them at risk of identity theft.
- Notifying the Consumer Protection Division of the NC Attorney General's Office if the breach affects more than 1,000 persons. Failure to do so may result in penalties under N.C.G.S. § 75-15.2. To notify the Attorney General of a breach go to www.noscamnc.com for the reporting form.

Please note that the requirements listed above are not exhaustive. Should your business need legal advice regarding compliance with the Identity Theft Protection Act of 2005, N.C.G.S. §§ 75-60, et seq., consult a private attorney for legal advice. The Attorney General's office cannot provide legal advice to individuals or individual businesses.