

Confidential Materials

1. Why must sensitive/confidential information be destroyed?

Answer: Identity Theft! How can someone steal your identity? By co-opting your name, Social Security Number, credit card number, or some other piece of your personal information for their own use. In short, identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. Here are some ways identity thieves work:

1. They open a new credit card account using your name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
2. They call your credit card issuer and, pretending to be you, change the mailing address on your credit card account. Then, your imposter runs up charges on your account. Because your bills are being sent to the new address, you may not immediately realize there's a problem.
3. They establish cellular phone service in your name.
4. They open a bank account in your name and write bad checks on that account.

2. Is there any legal protection from identity theft?

Answer: Yes! Identity Theft and Assumption Deterrence Act In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the problem of identity theft. Specifically, the Act amended 18 United States Code § 1028 to make it a federal crime when anyone **knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.**

Violations of the Act are investigated by federal investigative agencies such as the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service and prosecuted by the Department of Justice.

For more information on identity theft and how to minimize your personal risks visit the U.S. Governments, click on www.consumer.gov/idtheft/.

3. Is there any additional protection under North Carolina laws?

Answer: Yes! Article 19 C. Financial Identity Fraud NC General Statute 14-113.20 is quoted below.

§ 14-113.20. Financial Identity Fraud

(a) A person who knowingly obtains, possesses, or uses personal identifying information of another person without the consent of that other person, with the intent to fraudulently represent that the person is the other person for the purposes of making financial or credit transactions in the other person's name or for the purpose of avoiding legal consequences is guilty of a felony punishable as provided in General Statute 14-113.22(a).

(b) The term "identifying information" as used in this section includes the following:

1. Social security numbers.
2. Drivers license numbers.
3. Checking account numbers.
4. Savings account numbers.
5. Credit card numbers.
6. Debit card numbers.
7. Personal Identification (PIN) Code as defined in General Statute 14-113.8(6).
8. Electronic identification numbers.
9. Digital signatures.
10. Any other numbers or information that can be used to access a person's financial resources.

(c) It shall not be a violation under this section for a person to do any of the following:

1. Lawfully obtain credit information in the course of a bona fide consumer or commercial transaction.
2. Lawfully exercise, in good faith, a security interest or a right of offset by a creditor or financial institution.
3. Lawfully comply, in good faith, with any warrant, court order, levy, garnishment, attachment, or other judicial or administrative order, decree, or directive, when any party is required to do so. (1999-449, s. 1; 2000-140, s. 37.)

4. How do I determine if a document contains sensitive/confidential information?

Answer: Sensitive/confidential information includes the following:

Personal information

North Carolina State Government Agencies collect a great deal of information about individuals, and much of this information is quite sensitive. Records relating to motor vehicles, licensing of professions, trades, possible criminal activity, welfare, mental and physical health contain sensitive information.

Personnel files are a prime example of records containing personal information that have strict access/security restrictions while the records are active. This level of security should be maintained throughout the entire life of these records including during the destruction process.

Financial or commercially sensitive information

Records may contain information of a commercially sensitive nature. Examples include files containing information on an organization's financial position, tender bids, and any information that may give an unfair financial advantage to another.

Information given in confidence

Records may contain information that is given on condition that the information is not released. Examples include personal information and financial information, information

given by government agencies (foreign governments, interstate/federal bodies) and information from any source where the provider specifies that it is given in confidence.

Information relating to an investigation

Records relating to an investigation, usually into malpractice or criminal activity, may contain sensitive information. With such records, it is important to ensure that sensitive information is not released through inadequate or inappropriate destruction techniques.

Information posing a security risk

Records may contain information dealing with high security risk activities and premises. Examples of such records are plans of buildings for correctional institutions or banks, procedures for the delivery of large amounts of money, and security arrangements for movements of government officials.

5. How do I dispose of these sensitive/confidential documents?

Answer: Hire a Contractor to Destroy Documents.

If your agency or departments are considering contracting out the destruction of your records, it is your responsibility to ensure that destruction occurs in accordance with the approved methods of destruction. The contractor can collect records from your office for destruction, or you can deliver the records to them. A closed truck should be used whenever possible. However, if there is no alternative and the contractor can only provide an open truck, ensure that a cover secures the load. Sensitive and confidential records should only be conveyed in a closed and lockable vehicle.

Destruction of some confidential/sensitive information requires witnessing. If this is the case for you, check with the contractor to determine how this may be done.

If you are using a contractor to destroy records, always insist on a certificate of destruction. If records that were supposed to be destroyed are subsequently found, you could rightly point out that it was the contractor at fault, not your organization.

Make sure you know what method of destruction your contractor is using. You may want to request that the certificate of destruction note the method used. Some contractors may change their method of destruction based on an over supply of pulped paper or due to the cheaper costs of burying or dumping records.

And finally, be sure that all paper material that is destroyed through the shredding process is recycled.