

SECURITY BREACH NOTIFICATION CHART - North Carolina

N.C. Gen. Stat. [§§ 75-61, 75-65](#)

Effective December 1, 2005

S.B. 1048 (signed into law September 21, 2005)

Amended by S.B. 1017 (signed into law July 27, 2009)

Application. Any legal entity, however organized and whether or not organized to operate at a profit, but not including any government or governmental subdivision or agency (collectively, Entity) that owns or licenses PI of residents of NC or that conducts business in NC and owns or licenses PI in any form (computerized, paper, or otherwise).

Security Breach Definition. An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing PI where illegal use of the PI has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing PI along with the confidential process or key shall constitute a security breach.

- Good-faith acquisition of PI by an employee or agent of the Entity for a legitimate purpose is not a security breach, provided that the PI is not used for a purpose other than a lawful purpose of the Entity and is not subject to further unauthorized disclosure.

Notification Obligation. Any Entity to which the statute applies shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.

Notification to Consumer Reporting Agencies. If an Entity provides notice to more than 1,000 persons at one time pursuant to this section, the Entity shall notify, without unreasonable delay, all nationwide consumer reporting agencies of the timing, distribution, and content of the notice.

Attorney General Notification. In the event a business provides notice to an affected person pursuant to this section, the business shall notify without unreasonable delay the Consumer Protection Division of the state Attorney General's office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

Third-Party Data Notification. Any business that possesses records containing PI of residents of NC that the business does not own or license or conducts business in NC that possesses records containing PI that the business does not own or license, shall notify the owner or licensee of the PI of any security breach immediately following discovery of the breach.

Timing of Notification. The disclosure shall be made without unreasonable delay, consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the

reasonable integrity, security, and confidentiality of the data system.

Personal Information Definition. A person's first name or first initial and last name in combination with any of the following identifying information:

- Social Security number or employer taxpayer identification numbers;
- Driver's license, state identification card, or passport numbers;
- Checking account numbers;
- Savings account numbers;
- Credit card numbers;
- Debit card numbers;
- PINs;
- Digital signatures;
- Any other numbers or information that can be used to access a person's financial resources;
- Biometric data; or

Additionally, if (but only if) any of the following information "would permit access to a person's financial account or resources," it is considered PI when taken in conjunction with a person's first name, or first initial and last name:

- Electronic ID numbers;
- Email names or addresses;
- Internet account numbers;
- Internet ID names;
- Parent's legal surname prior to marriage; or

PI does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records

Notice Required. Notice must be clear, conspicuous, and shall include all of the following:

- A description of the incident in general terms;
- A description of the type of PI that was subject to the unauthorized access and acquisition;
- A description of the general acts of the business to protect the PI from further unauthorized access;
- A telephone number for the business that the person may call for further information and assistance, if one exists;
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;
- The toll-free numbers and addresses for the major consumer reporting agencies; and
- The toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the state Attorney General's office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

It may be provided by one of the following methods:

- Written notice;
- Telephonic notice, provided that contact is made directly with the affected persons; or
- Electronic notice, for those persons for whom it has a valid email address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. If the business demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to provide notice as required under the statute, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the Entity has email addresses for the subject persons;
- Conspicuous posting of the notice on the Entity's website, if the Entity maintains one; and
- Notification to major statewide media.

Exception: Compliance with Other Laws.

- **Interagency Guidance.** A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice shall be deemed to be in compliance.

Other Key Provisions:

- **Delay for Law Enforcement.** The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.
- **Attorney General Enforcement.** Civil and criminal penalties are available.
- **Private Right of Action.** An individual injured as a result of a violation of this section may institute a civil action.
- Waiver Not Permitted.