Security Breaches Under the NC Identity Theft Protection Act:
Basic Information for Local Health Departments

Jill Moore
UNC Institute of Government
April 2007

In 2005, the N.C. General Assembly passed a law requiring private businesses and government agencies to protect personally identifying information that could be used for identity theft. Parts of the law applied only to businesses (specifically defined to exclude government agencies), and other parts applied only to government agencies. Among many other things, the 2005 law required businesses, but not government agencies, to take specific actions when they experienced a security breach involving personally identifying information.

The Identity Theft Protection Act was amended in 2006 to make the parts of the law that deal with security breaches applicable to government agencies as well as businesses. As a result, government agencies that experience a "security breach" as defined in G.S. 75-61(14) must comply with G.S. 75-65, which specifies how to respond to a security breach.

Local health departments are subject to this requirement and therefore need to know:

- What constitutes a "security breach" under the NC Identity Theft Protection Act?
- If a health department experiences a security breach, what does the Act require it to do?

What is a "security breach"?

The duty to respond to a security breach is triggered only when an agency experiences an incident that meets the statutory definition of "security breach." See the appendix for the complete definition.

The key components of the definition of security breach are:

- There is an incident in which someone obtains unauthorized access to, and acquires, records or data.
- The records or data contain "personal information" that has not been encrypted or redacted. Personal data also has a statutory definition. It means:
    - A person's first name or initial and last name, PLUS
    - Any of the following information: social security or employer taxpayer identification number; drivers license, state identification card, or passport number; checking or savings account numbers; credit or debit card numbers; personal identification code or PINs; electronic identification numbers, e-mail names or addresses, Internet account numbers, or Internet identification names; digital signatures; any other numbers or information that can be used to access a person's financial resources; biometric data;

fingerprints; passwords; or the person's parent's legal surname prior to marriage.[1]

- And one of the following circumstances applies:
  - Illegal use of the personal information has occurred, or
  - Illegal use of the personal information is likely to occur, or
  - The unauthorized access and acquisition of the records or data creates a material risk of harm to a consumer

The definition of security breach also provides that:

- Unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key is a security breach.
- Good faith acquisition of personal information by an employee or agent for a legitimate purpose is not a security breach, so long as (1) the personal information is not used for an unlawful purpose and (2) the personal information is not subject to further unauthorized disclosure.

What does the Identity Theft Protection Act require a health department to do in response to a security breach?

If there has been a security breach, then the health department's basic duties are to:

- Determine the scope of the breach.
- Restore the security and confidentiality of the data system from which the breach occurred.
- Notify affected person(s) that there has been a security breach.
  - Notice must be provided without unreasonable delay, unless a law enforcement agency informs the government agency that providing notice may impede a criminal investigation or jeopardize national or homeland security.
  - The notice must be clear and conspicuous and include a description of the incident, the type of personal information that was subject to unauthorized access and acquisition, the agency's actions to protect the information from further unauthorized access, a telephone number the person may call for further information and assistance (if there is one), and a statement advising the person to remain vigilant by reviewing account statements and monitoring free credit reports.
  - The statute also specifies the acceptable methods for giving notice. In most cases, for health departments, it will probably be best to provide written notice.

[1] There may be circumstances in which disclosure of some of this information does not constitute a security breach. G.S. 75-65 provides that disclosure of the following information creates a security breach that an agency must respond to *only if* the information would permit access to the person's financial accounts or resources: electronic identification numbers, e-mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password.

Appendix:
N.C. Statutes Applicable to Government Agency Security Breaches

---

§ 132-1.10. Social security numbers and other personal identifying information.

… (c1) If an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, as defined in Article 2A of Chapter 75 of the General Statutes, the agency shall comply with the requirements of G.S. 75-65. …

G.S. § 75-61. Definitions.

The following definitions apply in this Article: …

(10) "Personal information". – A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information 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. …

(14) "Security breach". – An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information 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 personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

§ 14-113.20. Identity theft.

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

(1) Social security or employer taxpayer identification numbers.
(2) Drivers license, State identification card, or passport 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 G.S. 14-113.8(6).

(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

§ 75-65. Protection from security breaches.

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and 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. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

(c) 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 by this section 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.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(1) The incident in general terms.
(2) The type of personal information that was subject to the unauthorized access and acquisition.
(3) The general acts of the business to protect the personal information from further unauthorized access.
(4) A telephone number that the person may call for further information and assistance, if one exists.
(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.
(3) Telephonic notice provided that contact is made directly with the affected persons.
(4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($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 satisfy subdivisions (1), (2), or (3) of this subsection, 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:
a. E-mail notice when the business has an electronic mail address for the subject persons.
b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.
c. Notification to major statewide media.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.

(h) 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, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this section.

(i) A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

(j) Causes of action arising under this Article may not be assigned.