

GENERAL ASSEMBLY OF NORTH CAROLINA  
SESSION 2023

FILED SENATE  
Apr 6, 2023  
S.B. 733  
PRINCIPAL CLERK

S

D

SENATE BILL DRS55057-LR-103C

Short Title: Identity Theft Protection Act/Changes.

(Public)

Sponsors: Senators Chaudhuri, Mohammed, and Marcus (Primary Sponsors).

Referred to:

1 A BILL TO BE ENTITLED  
2 AN ACT AMENDING THE IDENTITY THEFT PROTECTION ACT.  
3 The General Assembly of North Carolina enacts:

4 **SECTION 1.** G.S. 75-61(14) reads as rewritten:

5 "(14) "Security breach". – An incident of unauthorized access to ~~and~~or acquisition  
6 of unencrypted and unredacted records or data containing personal  
7 information where illegal use of the personal information has occurred or is  
8 reasonably likely to occur or that creates a material risk of harm to a consumer.  
9 Any incident of unauthorized access to ~~and~~or acquisition of encrypted records  
10 or data containing personal information along with the confidential process or  
11 key shall constitute a security breach. Good faith acquisition of personal  
12 information by an employee or agent of the business for a legitimate purpose  
13 is not a security breach, provided that the personal information is not used for  
14 a purpose other than a lawful purpose of the business and is not subject to  
15 further unauthorized disclosure. Any determination that illegal use has not  
16 occurred or is not reasonably likely to occur or that no material risk of harm  
17 is created shall be documented and maintained for at least three years."

18 **SECTION 2.** G.S. 75-65 reads as rewritten:

19 "**§ 75-65. Protection from security breaches.**

20 (a) Any business that owns or licenses personal information of residents of North  
21 Carolina or any business that conducts business in North Carolina that owns or licenses personal  
22 information in any form (whether computerized, paper, or otherwise) shall ~~provide notice to the~~  
23 ~~affected person that there has been a security breach following discovery or notification of the~~  
24 ~~breach. The disclosure notification shall be made without unreasonable delay, consistent with the~~  
25 ~~legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent~~  
26 ~~with any measures necessary to determine sufficient contact information, determine the scope of~~  
27 ~~the breach and restore the reasonable integrity, security, and confidentiality of the data system.~~  
28 ~~For the purposes of this section, personal information shall not include electronic identification~~  
29 ~~numbers, electronic mail names or addresses, Internet account numbers, Internet identification~~  
30 ~~names, parent's legal surname prior to marriage, or a password unless this information would~~  
31 ~~permit access to a person's financial account or resources.~~do all of the following:

32 (1) Implement and maintain reasonable security procedures and practices,  
33 appropriate to the nature of the personal information and the size, complexity,  
34 and capabilities of the business, to protect the personal information from  
35 unauthorized access, destruction, use, modification, or disclosure.



- 1           (2) Provide notice to all persons affected by a security breach as soon as  
2 practicable, but not later than 45 days after discovery of the breach or reason  
3 to believe a breach has occurred in accordance with this section.
- 4           (3) Provide notice to the Consumer Protection Division of the Attorney General's  
5 Office that there has been a security breach as soon as practicable, but not later  
6 than 45 days after discovery of the breach or reason to believe a breach has  
7 occurred. The Consumer Protection Division may request any of the following  
8 information:
- 9           a. A description of the policies in place regarding breaches.  
10          b. Steps taken to rectify the breach.  
11          c. A copy of the police report, if relevant.  
12          d. A summary of the incident report.  
13          e. A summary of the computer forensics report, if a forensic examination  
14 was undertaken.  
15          f. All information prescribed under subsections (e) and (e1) of this  
16 section.

17           The business shall provide notification of a security breach in a manner consistent with the  
18 legitimate needs of law enforcement as provided in subsection (c) of this section and consistent  
19 with any measures necessary to determine sufficient contact information, to determine the scope  
20 of the breach, and to restore the reasonable integrity, security, and confidentiality of the data  
21 system. The information provided to the Consumer Protection Division of the Attorney General's  
22 Office pursuant to subdivision (3) of this subsection is not a public record as defined in  
23 G.S. 132-1.

24           For the purposes of this section, the term "personal information" does not include (i)  
25 electronic identification numbers or electronic mail names or addresses unless it includes any  
26 required security code, access code, or password that would allow access to an individual's  
27 financial account or resources or other personal information, as defined in this section, (ii)  
28 internet identification names, (iii) a parent's legal surname prior to marriage, or (iv) a password,  
29 unless the business is aware that this information would permit access to a person's financial  
30 account or resources or other personal information, as defined in this section.

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

38           (c) The notice required by this section shall be delayed if a law enforcement agency  
39 informs the business that notification may impede a criminal investigation or jeopardize national  
40 or homeland security, provided that such request is made in writing or the business documents  
41 such request contemporaneously in writing, including the name of the law enforcement officer  
42 making the request and the officer's law enforcement agency engaged in the investigation. The  
43 notice required by this section shall be provided ~~without unreasonable delay~~ within five days  
44 after the law enforcement agency communicates to the business its determination that notice will  
45 no longer impede the investigation or jeopardize national or homeland security.

46           (d) The notice shall be clear and conspicuous. The notice shall include all of the  
47 following:

- 48           (1) A description of the incident in general terms.  
49           (2) A description of the type of personal information that was subject to the  
50 unauthorized access and acquisition.

- 1 (3) A description of the general acts of the business to protect the personal  
2 information from further unauthorized access.
- 3 (4) A telephone number for the business that the person may call for further  
4 information and assistance, if one exists.
- 5 (5) Advice that directs the person to remain vigilant by reviewing account  
6 statements and monitoring free credit reports.
- 7 (6) The toll-free numbers and addresses for the major consumer reporting  
8 agencies.
- 9 (7) The toll-free numbers, addresses, and Web site addresses for the Federal Trade  
10 Commission and the North Carolina Attorney General's Office, along with a  
11 statement that the individual can obtain information from these sources about  
12 preventing identity theft.
- 13 (e) For purposes of this section, notice to affected persons may be provided by one of the  
14 following methods:
- 15 (1) Written notice.
- 16 (2) Electronic notice, for those persons for whom it has a valid e-mail address and  
17 with whom it regularly conducts business electronically or who have agreed  
18 to receive communications electronically if the notice provided is consistent  
19 with the provisions regarding electronic records and signatures for notices  
20 legally required to be in writing set forth in 15 U.S.C. § 7001.
- 21 (3) Telephonic notice provided that contact is made directly with the affected  
22 persons.
- 23 (4) Substitute notice, if the business demonstrates that the cost of providing notice  
24 would exceed two hundred fifty thousand dollars (\$250,000) or that the  
25 affected class of subject persons to be notified exceeds 500,000, or if the  
26 business does not have sufficient contact information or consent to satisfy  
27 subdivisions (1), (2), or (3) of this subsection, for only those affected persons  
28 without sufficient contact information or consent, or if the business is unable  
29 to identify particular affected persons, for only those unidentifiable affected  
30 persons. Substitute notice shall consist of all the following:
- 31 a. E-mail notice when the business has an electronic mail address for the  
32 subject persons.
- 33 b. Conspicuous posting of the notice on the Web site page of the  
34 business, if one is maintained.
- 35 c. Notification to major statewide media.
- 36 (e1) In the event a business provides notice to an affected person pursuant to this section,  
37 the business shall notify without unreasonable delay the Consumer Protection Division of the  
38 Attorney General's Office of the nature of the breach, the number of consumers affected by the  
39 breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future,  
40 and information regarding the timing, distribution, and content of the notice.
- 41 ~~(f) In the event a business provides notice to more than 1,000 persons at one time~~  
42 ~~pursuant to this section, the business shall notify, without unreasonable delay, the Consumer~~  
43 ~~Protection Division of the Attorney General's Office and all consumer reporting agencies that~~  
44 ~~compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. §~~  
45 ~~1681a(p), of the timing, distribution, and content of the notice.~~
- 46 (g) Any waiver of the provisions of this Article is contrary to public policy and is void  
47 and unenforceable.
- 48 (g1) A person or agency that is subject to and in compliance with the Health Insurance  
49 Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, as amended and with  
50 regulations promulgated under that act, shall be deemed in compliance with this section. If notice

1 of a security breach is provided to any affected person or agency pursuant to HIPAA, then notice  
2 shall also be provided to the Consumer Protection Division in the Office of the Attorney General.

3 (h) A financial institution that is subject to and in compliance with the Federal  
4 Interagency Guidance Response Programs for Unauthorized Access to Consumer Information  
5 and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve  
6 System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the  
7 Currency, and the Office of Thrift Supervision; or a credit union that is subject to and in  
8 compliance with the Final Guidance on Response Programs for Unauthorized Access to Member  
9 Information and Member Notice, issued on April 14, 2005, by the National Credit Union  
10 Administration; and any revisions, additions, or substitutions relating to any of the said  
11 interagency guidance, shall be deemed to be in compliance with this section.

12 (h1) If a consumer receives notice under this section or is the subject of a security breach  
13 by a consumer reporting agency, and the consumer's personal information was held by a  
14 consumer reporting agency, then that consumer reporting agency shall offer to provide  
15 appropriate identity theft prevention and mitigation services such as credit monitoring at no cost  
16 to the consumer for not less than 24 months. The consumer reporting agency shall provide the  
17 consumer with information necessary to take advantage of the offer.

18 (h2) If a business knows or has reason to know that said business experienced a security  
19 breach that requires notice under this section and the security breach includes a person's social  
20 security number, the business shall contract with a third party to offer to each person whose social  
21 security number was disclosed in the security breach, or is reasonably believed to have been  
22 disclosed in the security breach, credit monitoring services at no cost to the person for a period  
23 of not less than 24 months.

24 (h3) A consumer reporting agency shall not knowingly offer a paid product to prevent  
25 unauthorized access or restrict access to a consumer's credit unless, at the time of the transaction,  
26 the consumer reporting agency (i) notifies the consumer of the availability of obtaining a security  
27 freeze without charge and (ii) provides information to the consumer on how to obtain a security  
28 freeze.

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

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

33 **SECTION 3.** G.S. 75-66 reads as rewritten:

34 "**§ 75-66. Publication of personal information.**

35 (a) It shall be a violation of this section for any person to knowingly broadcast or publish  
36 to the public on radio, television, cable television, in a writing of any kind, or on the Internet, the  
37 personal information of another with actual knowledge that the person whose personal  
38 information is disclosed has previously objected to any such disclosure.

39 (b) As used in this section, "person" means any individual, partnership, corporation, trust,  
40 estate, cooperative, association, or other entity, but does not include any:

41 (1) Government, government subdivision or agency.

42 (2) Entity subject to federal requirements pursuant to the Health Insurance  
43 Portability and Accountability Act (HIPAA).

44 (c) ~~As used in this section, the phrase "personal information" includes a person's first~~  
45 ~~name or first initial and last name in combination with any of the following information:~~

46 (1) ~~Social security or employer taxpayer identification numbers.~~

47 (2) ~~Drivers license, State identification card, or passport numbers.~~

48 (3) ~~Checking account numbers.~~

49 (4) ~~Savings account numbers.~~

50 (5) ~~Credit card numbers.~~

51 (6) ~~Debit card numbers.~~

- 1           (7) ~~Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).~~  
2           (8) ~~Digital signatures.~~  
3           (9) ~~Any other numbers or information that can be used to access a person's~~  
4           ~~financial resources.~~  
5           (10) ~~Biometric data.~~  
6           (11) ~~Fingerprints.~~  
7           (12) ~~Passwords.~~

8           (c1) For the purposes of this section, the phrase "personal information" does not include  
9 any of the following:

- 10           (1) Electronic identification numbers or electronic mail names or addresses unless  
11 it includes any required security code, access code, or password that would  
12 allow access to an individual's financial account or resources or other personal  
13 information, as defined in G.S. 75-61(10).  
14           (2) Internet identification names.  
15           (3) A parent's legal surname prior to marriage.  
16           (4) A password, unless the business is aware that this information would permit  
17 access to a person's financial account or resources or other personal  
18 information, as defined in G.S. 75-61.

19           (d) Nothing in this section shall:

- 20           (1) Limit the requirements or obligations under any other section of this Article,  
21 including, but not limited to, G.S. 75-62 and G.S. 75-65.  
22           (2) Apply to the collection, use, or release of personal information for a purpose  
23 permitted, authorized, or required by any federal, State, or local law,  
24 regulation, or ordinance.  
25           (3) Apply to data integration efforts to implement the State's business intelligence  
26 strategy as provided by law or under contract.

27           (e) Any person whose property or person is injured by reason of a violation of this section  
28 may sue for civil damages pursuant to the provisions of G.S. 1-539.2C."

29           **SECTION 4.** Article 2A of Chapter 75 of the General Statutes is amended by adding  
30 a new section to read:

31 **"§ 75-67. Consumer report consent.**

32 A person shall not obtain, use, or seek the consumer report or credit score of a consumer in  
33 connection with an application for credit unless the user obtains the written, verbal, or electronic  
34 consent of the consumer, as appropriate to the manner in which the application for credit is  
35 made."

36           **SECTION 5.** G.S. 14-113.20(b) reads as rewritten:

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

- 38           (1) Social security or employer taxpayer identification numbers.  
39           (2) Drivers license, State identification card, or passport numbers.  
40           (3) Checking account numbers.  
41           (4) Savings account numbers.  
42           (5) Credit card numbers.  
43           (6) Debit card numbers.  
44           (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).  
45           (8) Electronic identification numbers, electronic mail names or addresses,  
46 Internet account numbers, or Internet identification names.  
47           (9) Digital signatures.  
48           (10) Any other numbers or information that can be used to access a person's  
49 financial resources.  
50           (11) Biometric data.  
51           (12) Fingerprints.

- 1 (13) Passwords.
- 2 (14) Parent's legal surname prior to marriage.
- 3 (15) Health insurance policy number, subscriber identification number, or any
- 4 other unique identifier used by a health insurer or payer to identify the person.
- 5 (16) Any information regarding the individual's medical history or condition,
- 6 medical treatment or diagnosis, or genetic information, by a health care
- 7 professional."

8 **SECTION 6.** This act is effective when it becomes law.