



BILL SUMMARY

SF 2308 Identity Theft Notice of Security Breach

Status of Bill: House Calendar (passed Senate 48-0)
Committee: Commerce (passed 23-0)
Floor Manager: Rep. Doris Kelley
Research Analyst: Tom Patterson 281-5159 thomas.patterson@legis.state.ia.us

April 2, 2008

SF 2308 requires notification of Iowa consumers of a security breach involving personal information by the person who owns, maintains or otherwise possesses the information.

Consumer Notification Security Breach:

1. The notice requirement applies to any person who owns, maintains, or otherwise possesses data used the course of the person's business, vocation, occupation, or volunteer activities, that includes a consumer's personal information
2. The notice requirement also applies to any person who maintains or otherwise possesses personal information on behalf of another person – such as a list management company that maintains subscription information on behalf of a magazine.
 - If there is a breach of security, this person notifies the owner or licensor of the information immediately following discovery, who is then responsible for notifying consumers.
3. Notice shall be provided to consumers whose personal information is included upon discovery of the security breach, or upon receipt of notice from another person, as described in paragraph 2.
4. Notice shall be in the most expeditious manner possible, without unreasonable delay, consistent with legitimate law enforcement needs, and consistent with measures to determine consumer contact information, the scope of the breach, and to restore data integrity, security, and confidentiality.
 - Notice may be delayed upon written request of a law enforcement agency that it will impede a criminal investigation. Notice shall then be made after the agency informs the person in writing that the notice will not compromise the investigation.
5. Notice is not required if, after appropriate investigation or consultation with the relevant federal, state, or local law enforcement agencies, the person determines that no reasonable likelihood of harm to the consumers has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years.
 - Notice does not apply to any of the following:
 - A person who complies with notice or breach of security procedures in a state law, federal law, or regulations of the persons primary or functional federal regulator that provide greater protection to personal information and at least as thorough a disclosure as this Act.
 - A person who is subject to and complies with regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. } 6801-6809.

Method of Notification. Notification to the consumer may be by:

1. Written notice.
2. Electronic notice, if this is the customary method of communication with the consumer or is consistent with provisions regarding electronic records and signatures in chapter 554D and the federal Electronic Signatures in Global and National Commerce Act.

3. Substitute notice, if the person demonstrates that providing notice would cost over \$250,000, that the affected class of consumers exceeds 350,000 persons, or that the person lacks sufficient contact information, then substitute notice shall consist of the following:
 - Email when the person has an email address for the affected consumers.
 - Conspicuous posting of the notice or a link to the notice on the person's internet web site..
 - Notification to major statewide media.
4. Contents of Notice: The notice shall include, at a minimum, all of the following:
 - A description of the security breach.
 - The approximate date of the security breach .
 - The type of personal information obtained as a result of the security breach.
 - Contact information for consumer reporting agencies.
 - Advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general.

"Breach of security" means unauthorized acquisition of personal information maintained that compromises the security, confidentiality, or integrity of that information.

1. Not A Breach of Security. Good faith acquisition of personal information by a person or their employee or agent for a legitimate purpose, if the personal information is not used in violation of the law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
2. Not A Breach of Security. Transmittal or reception of personal information on a radio broadcasting system operated pursuant to section 80.9, subsection 2, paragraph "e", or any similar radio broadcasting system, utilized by a federal, state, or local law enforcement agency, by an officer or employee of a federal, state, or local law enforcement agency, or by an emergency medical care provider as defined in section 147A.1, subsection 4, in the performance of official duties.

"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements relating to the individual, if the data elements are not encrypted, redacted (only last 4 digits accessible), or otherwise altered in such a manner that the name or data elements are unreadable:

1. Social security number.
2. Driver's license number or other unique ID number created or collected by a government body.
3. Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's account.
4. Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
5. Unique biometric data, such as a fingerprint, voice print or recording, retina or iris image, or other unique physical representation or digital representation of biometric data.
6. This does not include information lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.

Violations / Remedies. Violation are unlawful practices pursuant to the Iowa Consumer Fraud Law (714.16). In addition to remedies provided the Attorney General under 714.16, subsection 7, the Attorney General may seek and obtain an order that a violator pay damages to the Attorney General on behalf of the injured person. These rights and remedies are cumulative to each other and to any other rights and remedies available under the law.

AMENDMENT SUMMARY

H-8323 by the Commerce Committee: The amendment makes the following technical changes:

1. Clarifies that a breach of security applies to personal information maintained in computerized form.
2. Strikes the following exception to the definition of breach of security: *“Transmittal or reception of personal information on a radio broadcasting system operated pursuant to section 80.9, subsection 2, paragraph “e”, or any similar radio broadcasting system, utilized by a federal, state, or local law enforcement agency, by an officer or employee of a federal, state, or local law enforcement agency, or by an emergency medical care provider as defined in section 147A.1, subsection 4, in the performance of official duties.”*
3. The bill’s definition of “personal information” includes biometric data, which is a *“fingerprint, voice print or recording, retina or iris image, or other unique physical or digital representation of biometric data.”* The amendment strike “voice print or recording” from the definition.
4. The amendment changes a reference from to a person “who was subject to a breach of security” to “that was subject to a breach of security”.
5. Regarding allowable methods of notification, the bill refers to “written notice”, which the amendment changes to “written notice to the last available address the person has on the person’s records.”
6. The bill states that no notice is required if after an investigation or consultation with a law enforcement agency, the entity determines that there is “no reasonable likelihood of harm to the consumers”. The amendment changes this to “no reasonable likelihood of financial harm to the consumers”.

H-8352 by Granzow (R-Hardin) – Office of Citizens’ Aide Report on Government Security

Breaches: The amendment does the following:

1. Requires a government or government subdivision that, under the terms of the bill, must notify consumers of a security breach of information they own, maintain or possess, must also send a written notice of the security breach to the Office of the Citizens’ Aide.
2. Requires the Office of the Citizens’ Aide to annually file a report with the General Assembly and the Governor concerning all such notices it receives.
 - The report shall not disclose the name or personal information of any affected individual.
 - If the report criticizes a named agency or official, it shall also include unedited replies to the criticism by the agency or official, unless excused by the agency or official.

H-8353 by Tjepkes (R-Webster) – Disclosure of Records By a Public Official – Criminal Penalty:

The amendment states that, unless otherwise authorized by state or federal law, a public official in possession or control of personal information who intentionally discloses that information for compensation is guilty of a Class “D” felony (imprisonment for up to 5 years and a fine of from \$750 to \$7,500).

- “Compensation” means any money, thing of value, or financial benefit conferred to a public official by a person other than the government body that employs the public official.
- “Public Official” means an official or employee of the state or a local government, or an elected official of the state or a local government.
- “Personal Information” is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if neither the name nor the data elements are encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
 - Social security number.
 - Driver's license number or other unique identification number created or collected by a government body.

- Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password.
- Unique biometric data, such as a fingerprint, voice print or recording, retina or iris image, or other unique physical representation or digital representation of the biometric data.

H-8376 to H-8353 by Kelley (D-Black Hawk) – Definition of Personal Information: The amendment, for consistency, strikes the definition of “personal information” in the Tjepkes amendment and replaces it with a reference to the definition of “personal information” created by the bill.

H-8356 by Pettengill (R-Benton) – Destruction of Public Records of Personal Information: The amendment requires, unless otherwise required by federal or state law, each government body to take reasonable steps to destroy or arrange for the destruction of a public record, or portion thereof, containing personal information within its control, that no longer needs to be maintained. Destruction shall be in accordance with the following minimum standards:

- Paper documents with personal information shall be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed.
- Electronic media and other nonpaper media with personal information shall be destroyed or erased so that personal information cannot practicably be read, reconstructed, or deciphered through any means.

A government body may contract with a third party to destroy these records in accordance with these requirements. Any third party shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to, acquisition of, or use of personal information during the collection, transportation, and destruction of personal information.

A government body or third party that violates these provisions shall be subject to civil penalty of not more than \$100 per record affected, up to a maximum \$50,000 per incident. The Attorney General or a county attorney may enforce these provisions.

- “Personal information” is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if neither the name nor the data elements are encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:
 - Social security number.
 - Driver's license number or other unique identification number created or collected by a government body.
 - Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.
 - Unique electronic identifier or routing code, in combination with any required security code, access code, or password.
 - Unique biometric data, such as a fingerprint, voice print or recording, retina or iris image, or other unique physical representation or digital representation of the biometric data.

H-8365 by Kelley (D-Black Hawk) – Technical Change to Notice Requirements:

1. The bill's notice requirement applies to any person who *owns, maintains, or otherwise possesses* data used in the course of the person's business, vocation, occupation, or volunteer activities, that includes a consumer's personal information.
 - The amendment strikes “maintains, or otherwise possesses” as this is covered in the provision described below, and adds “or licenses computerized” data, to be consistent with the provision described below.
2. The bill's notice requirement also applies to any person who maintains or otherwise possesses personal information on behalf of another person – such as a list management company that maintains subscription information on behalf of a magazine. If there is a breach of security, this person notifies the owner or licensor of the information immediately following discovery, who is then responsible for notifying consumers.