Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - District of Columbia

D.C. Code § 28-3851 ***et seq.***

Council Bill 16-810 (signed into law March 8, 2007)

Effective July 1, 2007

Council Bill 23-0215 (signed into law March 26, 2020)

Effective June 17, 2020

Application. Any person or entity (collectively, Entity) who conducts business in D.C. and who, in the course of such business, owns or licenses computerized or other electronic data that includes PI.

Security Breach Definition. An unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of PI maintained by the Entity.

- Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.
- Good-faith acquisition of PI by an employee or agent of the Entity for the purposes of the Entity is not a breach of the security of the system if the PI is not used improperly or subject to further unauthorized disclosure.
- Acquisition of personal information of an individual that the Entity reasonably determines, after a reasonable investigation and consultation with the Office of the Attorney General and federal law enforcement agencies, will likely not result in harm to the individual, is not a breach.

Notification Obligation. An Entity to which the statute applies, and that discovers a breach of the security system shall promptly notify any D.C. resident whose PI was included in the breach.

Notification to Consumer Reporting Agencies. If any Entity is required to notify more than 1,000 persons of a breach of security, the Entity shall also notify, without unreasonable delay, all nationwide consumer reporting agencies, of the timing, distribution, and content of the notices. This subsection shall not apply to an Entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act.

Attorney General/Agency Notification. If 50 or more residents are affected, the Entity must notify the Attorney General as expeditiously as possible and without unreasonable delay, and no later than when individual notice is sent.

The notice must include:

- Name and contact information of the person or entity reporting the breach;
- Name and contact information of the person or entity that experienced the breach;
- The nature of the breach of the security of the system;
- Types of personal information compromised by the breach;
- Number of District residents affected by the breach;

- Cause of the breach, including the relationship between the person or entity that experienced the breach and the person responsible for the breach, if known;
- Remedial action taken, to include steps taken to assist District residents affected by the breach;
- Date and time frame of the breach, if known;
- Address and location of corporate headquarters, if outside of the District;
- Any knowledge of foreign country involvement; and
- Sample of the notice to be provided to District residents.

Third-Party Data Notification. Any Entity that maintains, handles, or otherwise possesses computerized or other electronic data that includes PI that the Entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery.

Timing of Notification. In the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal Information Definition. (i) An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information:

- Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
- Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account;
- Medical information;
- Genetic information and deoxyribonucleic acid profile;
- Health insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information;
- Biometric data of an individual generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that is used to uniquely authenticate the individual's identity when the individual accesses a system or account; or
- Any combination of data elements included in the above bullet points that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier.

(ii) Username or email address in combination with a password, security question and answer, or other means of authentication, or any combination of data elements included in the above bullet points, that permits access to an individual's email account.

PI shall not include information that is lawfully made available to the general public from federal, state, or local government records

Notice Required. Notice may be provided by one of the following methods:

- Written notice; or

- Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act)

Notice shall include:

- Categories of information accessed
- Contact information for Entity making notification
- Contact information for consumer reporting agencies, the FTC, and Office of the Attorney General

Credit Monitoring Services. When the breach is reasonably believed to include a social security number or taxpayer identification number, the Entity shall offer to each resident whose social security number or tax identification number was released identity theft protection services at no cost to such resident for at least 18 months.

Substitute Notice Available. If the Entity demonstrates that the cost of providing notice to persons would exceed $50,000, that the number of persons to receive notice under the statute exceeds 100,000, or that the Entity does not have sufficient contact information. Substitute notice shall consist of all of the following:

- Email notice when the Entity has email addresses for the subject persons;
- Conspicuous posting of the notice on the website of the Entity, if the Entity maintains one; and
- Notice to major local and, if applicable, national media.

Exception: Compliance with Other Laws. An Entity that maintains procedures for a breach notification system under the GLBA, HIPAA, or HITECH, and provides notice in accordance with such Acts, and any rules, regulations, guidance and guidelines thereto, to each affected resident in the event of a breach, shall be deemed to be in compliance with the law with respect to the notification of affected individuals. The Entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
- **Attorney General Enforcement.** The Attorney General may seek direct damages and injunctive relief.
- **Private Right of Action.** Any D.C. resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering.
- Waiver Not Permitted.