

# Washington DC

D.C. Code § 28-3851 *et seq.*

## Quick Links

---

[Statute](#)

[AG Website](#)

## Quick Facts

---

Is “Personal Information” broader than the general definition? <sup>1</sup>	✓ Yes
Does the law apply to paper records?	✗ No
Is notification triggered by access only?	✗ No
Is a risk-of-harm analysis permitted?	✓ Yes
Is notice to a state agency or AG required?	✓ Yes, if more than 50 residents notified
Is there a specific deadline for individual notices?	✗ No
Is there a specific format or language that must be included in the individual notice?	✓ Yes
Is a private right of action permitted?	✓ Yes

## “Breach” Definition

---

The unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information maintained by the person or entity who conducts business in the District of Columbia.

## “Personal Information” Definition

---

1. An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following:
  - a. 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

<sup>1</sup> The general definition of “Personal Information” is an individual's name in combination with any one or more of the following: (1) Social Security number; (2) driver's license number or state identification card number; or (3) a financial account number or credit or debit card number in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account.

- b. 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
- c. Medical information
- d. Genetic information and deoxyribonucleic acid profile
- e. 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
- f. Biometric data to uniquely authenticate the individual's identity when the individual accesses a system or account, or
- g. Any combination of the above-data elements to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier

Or

- 2. A username or e-mail 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 that permits access to an individual's e-mail account.

### Notification Trigger

---

Following discovery or notification of the breach:

- 1. Entity that owns or licenses personal information shall disclose the breach to each state resident in the most expedient time possible and without unreasonable delay, after the discovery or notification,
- 2. Entity that does not own or have the right to license the personal information shall notify the owner or licensee immediately following discovery of the breach.

### Risk-of-Harm Analysis Standard

---

Notice is not required if a determination is made after reasonable investigation and consultation with the Attorney General and federal law enforcement that the acquisition of PI will likely not result in harm to the individual.

### Special Form/Content of Consumer Notice

---

The notice shall include:

- 1. To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including the elements of personal information that were, or are reasonably believed to have been, acquired
- 2. Contact information for the person or entity making the notification, including the business address, telephone number, and toll-free telephone number if one is maintained
- 3. The toll-free telephone numbers and addresses for the major consumer reporting agencies and information how a resident may request a security freeze; and
- 4. The toll-free telephone numbers, addresses, and website addresses for the following entities, including a statement that an individual can obtain information from these sources about steps to take to avoid identity theft:

- a. The Federal Trade Commission; and
  - b. The Office of the Attorney General for the District of Columbia.
5. If the entity maintains procedures for notification under the GLBA, HIPAA, or HITECH and provides notice in accordance with those sections, the entity is deemed in compliance with the provisions for providing notice to consumers.

### **AG Notice Trigger/Deadline**

---

Notice must be provided to the Attorney General, made in the most expedient manner possible and without unreasonable delay, if the breach affects more than 50 District residents.

The notice must include:

1. The name and contact information of the person or entity reporting the breach
2. The name and contact information of the person or entity that experienced the breach
3. The nature of the breach of the security of the system, including the name of the person or entity that experienced the breach
4. The types of personal information compromised by the breach
5. The number of District residents affected by the breach
6. The 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
7. The remedial action taken by the person or entity to include steps taken to assist District residents affected by the breach
8. The date and time frame of the breach, if known
9. The address and location of corporate headquarters, if outside of the District
10. Any knowledge of foreign country involvement, and
11. A sample of the notice to be provided to District residents.

### **Notification to Consumer Reporting Agencies Threshold**

---

In the event the entity provides notice to more than 1,000 consumers at one time, the data collector shall notify, without unreasonable delay, all consumer reporting agencies.