D.C. Code § 28-3852

The Official Code is current through March 22, 2024

District of Columbia Official Code > Division V. Local Business Affairs. (Titles 25 — 37) > Title 28. Commercial Instruments and Transactions. (Subts. I — II) > Subtitle II. Other Commercial Transactions. (Chs. 21 — 54) > Chapter 38. Consumer Protections. (Subchs. I — IV) > Subchapter II. Consumer Security Breach Notification. (§§ 28-3851 — 28-3853)

§ 28-3852. Notification of security breach.

(a) Any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(a-1) The notification required under subsection (a) of this section 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, including a statement notifying the resident of the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1 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.

(a-2) Notwithstanding subsection (a-1) of this section, in the case of a breach of the security of the system that only involves personal information as defined in § 28-3851(3)(A)(ii), the person or entity may comply with this section by providing the notification in electronic format or other form that directs the person to change the person's password and security question or answer, as

applicable, or to take other steps appropriate to protect the e-mail account with the person or entity and all other online accounts for which the person whose personal information has been breached uses the same username or email address and password or security question or answer.

(b) Any person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or 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.

(b-1) In addition to giving the notification required under subsection (a) of this section, and subject to subsection (d) of this section, the person or entity required to give notice shall promptly provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia if the breach affects 50 or more District residents. This notice shall be made in the most expedient manner possible, without unreasonable delay, and in no event later than when notice is provided under subsection (a) of this section. The written notice shall 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.

(b-2) The notice required under subsection (b-1) of this section shall not be delayed on the grounds that the total number of District residents affected by the breach has not yet been ascertained.

(c) If any person or entity is required by subsection (a) or (b) of this section to notify more than 1,000 persons of a breach of security pursuant to this subsection, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by section 603(p) of the Fair Credit Reporting Act, approved October 26, 1970 (84 Stat. 1128; 15 U.S.C. § 1681a(p)), of the timing, distribution and content of the notices. Nothing in this subsection shall be construed to require the person to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients. This subsection shall not apply to a person or entity who is required to notify consumer reporting agencies of a breach pursuant to Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 et seq[.]).

(d) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation but shall be made as soon as possible after the law enforcement agency determines that the notification will not compromise the investigation.

(e) [Repealed].

(f) A waiver of any provision of this subchapter shall be void and unenforceable.

(g) A person or entity that maintains procedures for a breach notification system under Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 et seq.), or the breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability Accountability Act of 1996, approved August 21, 1996 (Pub. L. No. 104-191; 110 Stat. 1936), or the Health Information Technology for Economic and Clinical Health Act, approved February 17, 2009 (Pub. L. No. 111-5; 123 Stat. 226), 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 this section with respect to the notification of residents whose personal information is included in the breach. The person or entity shall, in all cases, provide written notice of the breach of the security of the system to the Office of the Attorney General for the District of Columbia as required under subsection (b-1) of this section.

History

(Mar. 8, 2007, D.C. Law 16-237, § 2(c), 54 DCR 393; June 17, 2020, D.C. Law 23-98, § 2(a)(4), 67 DCR 3923.)