

**COUNCIL OF THE DISTRICT OF COLUMBIA
COMMITTEE OF THE WHOLE
DRAFT COMMITTEE REPORT**

1350 Pennsylvania Avenue, NW, Washington, DC 20004

TO: All Councilmembers

FROM: Chairman Phil Mendelson
Committee of the Whole

DATE: January 21, 2020

SUBJECT: Report on Bill 23-215, the “Security Breach Protection Amendment Act of 2020”

The Committee of the Whole, to which Bill 23-215, the “Security Breach Protection Amendment Act of 2020” was referred, reports favorably thereon, with amendments, and recommends approval by the Council.

CONTENTS

I.	Background and Need.....	1
II.	Legislative Chronology.....	7
III.	Position of the Executive	7
IV.	Comments of Advisory Neighborhood Commissions	7
V.	Summary of Testimony.....	7
VI.	Impact on Existing Law	9
VII.	Fiscal Impact.....	10
VIII.	Section-by-Section Analysis.....	10
IX.	Committee Action.....	12
X.	Attachments	12

I. BACKGROUND AND NEED

Bill 23-215, the “Security Breach Protection Amendment Act of 2020”¹ was introduced by Chairman Phil Mendelson at the request of the Attorney General on March 21, 2019. The bill expands the definition of personal information; adds additional requirements for the contents of a notification of a security breach to consumers; requires notification of a breach to the Office of Attorney General; requires persons and entities that possess personal information to implement and maintain reasonable security procedures and practices; and requires a company to provide 18 months of identity theft protections to an individual if his or her social security number or tax identification number is part of the security breach. Finally, the bill makes a violation of the data breach law a violation of the District’s Consumer Protection Procedures Act.

Bill 23-215, if approved, will be the first update to the District’s data breach law since the

¹ The title of the bill has been updated to reflect that the bill was introduced in 2019 but is being considered by the Council in 2020.

Consumer Personal Information Security Breach Notification Act² was approved by the Council and became law in 2007. Since that time the District's law has not kept up with today's technology and is inadequate when compared to laws in other states. Ms. Wilkins from the Office of the Attorney General (OAG) testified at the hearing on Bill 23-215, that the District has fallen behind, and District consumers are not being sufficiently protected.³ She added that in the new digital era there is more data collected on consumers, and the more data that is collected the more attractive it becomes to those who want to misuse that data.⁴ In fact, the District had the highest cases per capita of identity theft and fraud when compared to others states.⁵

In recent years there have been numerous significant data breaches where the personal information of District residents was improperly acquired. In 2017, the breach of personal information maintained by Equifax comprised data belonging to 143 million Americans, which included more than 350,000 District residents.⁶ It was reported in 2018 that Facebook believed that over 345,000 District residents information may have been improperly shared in the Cambridge Analytica personal privacy breach.⁷ Target had to pay \$18.5 million to 47 states and the District of Columbia as part of a settlement agreement over a security breach in 2013 that compromised the data of millions of consumers.⁸

Justin Brookman from Consumer Reports testified at the hearing on Bill 23-215 that these data breaches are causing consumers to lack confidence in institutions to keep their data safe from misuse.⁹ Bill 23-215 intends restore consumer confidence by protecting District residents from bad actors by incentivizing companies to take the necessary steps to safeguard their personal information. Moreover, the new notification requirements in the bill provide more information and clarity to consumers so they can make the most informed decision to best protect themselves.

Personal Identifiable Information

Bill 23-215 expands the definition of the term "personal information" to add additional sensitive information that was not contemplated when the current law was adopted over ten years ago. The update ensures that the District's law aligns with the growing amount of personal data

² Effective March 8, 2007 (D.C. Law 16-237; D.C. Official Code § 28-3851 *et seq.*).

³ Elizabeth Wilkins, Senior Counsel, Office of the Attorney General, Testimony before the DC Council Committee of the Whole, 3, November 12, 2019.

⁴ *Id.* at 2.

⁵ See Brian Young, Public Policy Manager, National Consumers League, Testimony before the DC Council Committee of the Whole, 2, November 12, 2019.

⁶ See Press Release, Karl Racine, Attorney General for the District of Columbia, Attorney General Racine Recommends District Residents Take Precautions in the Wake of Equifax Data Breach (Sept. 8, 2017), <https://oag.dc.gov/release/attorney-general-racine-recommends-district>.

⁷ See Mike Valerio, Facebook: Half of DC potentially exposed to Cambridge Analytica Hack (May 3, 2018), <https://www.wusa9.com/article/news/local/dc/facebook-half-of-dc-potentially-exposed-to-cambridge-analytica-hack/65-548466144>.

⁸ See Rachel Abrams, Target to Pay \$18.5 Million to 47 States in Security Breach Settlement, The New York Times (March 23, 2017), <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>.

⁹ Justin Brookman, Director, Consumer Privacy and Technology Policy, Consumer Reports, Testimony before the DC Council Committee of the Whole, 4, November 12, 2019.

that could be improperly acquired.¹⁰ The Committee believes expanding the definition is a step in the right direction since the current law is inadequate. For instance, under the current law a resident would not have to be notified if: his or her email account was breached; information about his or her health insurance information is improperly disclosed; or information about his or her medical history, biometric data, or DNA profile is acquired by a bad actor. As Mr. Brookman stated at the hearing, this is common-sense legislation that would better protect the privacy and financial security of District residents.¹¹

Of note, the Committee, working with the OAG, updated the Committee Print for Bill 23-215 to address concerns that the definition for the term “personal information”, as proposed, was too broad and vague. The Committee believes the definition in the Committee Print strikes the right balance between protecting consumers and providing clarity for businesses to be able to follow the requirements in the law.

Risk of harm analysis

During the hearing on Bill 23-215, Ms. Critides from the State Privacy & Security Coalition testified that the Council should consider adding a risk of harm analysis that triggers notification to consumers. She indicated that a majority of state breach notice laws only require notification if there is a risk of harm to a consumer.¹² This is an important criterion because it avoids “de-sensitizing” residents from receiving notices from technical breaches that pose no risk to them.¹³

Companies should be as transparent as possible to the public when there is a data breach. However, the Committee is concerned that unnecessary notifications of a data breach that cause no harm to a consumer might numb the consumer and may threaten the amount of attention the consumer will pay to a breach where there could be a significant risk of harm.¹⁴ The Committee wants to ensure that when a consumer receives a notification of a breach that they take the notification seriously and take the necessary steps to protect themselves from harmful purposes, such as identity theft or fraud.

Taken into account the importance of transparency and ensuring that consumers are not inundated with unnecessary notifications, the Committee Print for Bill 23-215 provides that it is not considered a breach of the security of the system if the company, after consulting with law enforcement officials, reasonably determines that the breach will not harm the consumer.¹⁵

¹⁰ See *Supra* note 3 at 4.

¹¹ *Supra* note 9 at 2.

¹² Elaine Critides, Counsel, State Privacy & Security Coalition, Testimony before the DC Council Committee of the Whole, 2, November 12, 2019.

¹³ See *Id.*

¹⁴ See also *Security Breach Notification Laws: Views from Chief Security Officers*, University of California-Berkeley School of Law 34 (December 2007), https://www.law.berkeley.edu/files/cso_study.pdf.

¹⁵ The Committee modeled the language in the Committee Print on Connecticut’s data breach law. Conn. Gen. Stat. § 36a-701b(b)(1), provides that “notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably

Requiring coordination with District and federal law enforcement agencies will assure a consumer that his or her data is sufficiently protected. Adding in this provision also builds on the safe harbor requirements that are already provided in the current law.¹⁶

Notification Requirements

Bill 23-215 inserts requirements for the type of information that must be provided by a company when a District resident is notified that his or her personal information has been improperly disclosed. Current law does not specify the type of information that must be included in the breach notification.¹⁷ The specificity required in the notification will ensure that consumers are armed with information that they need to protect themselves.¹⁸

The Committee has heard concerns that the notification requirements for email password breaches should be different. This is due to the fact that the only recourse in these cases is to have a consumer update his or her password for their email account and other online accounts. Ms. Critides testified at the hearing on Bill 23-215, that this separate notification requirement should be added in the bill to help avoid sending irrelevant breach notifications that could confuse District residents.¹⁹ Hearing the concerns, the Committee Print for Bill 23-215 includes a separate notification requirement for email password breaches similar to the law in California.²⁰

Further, Bill 23-215, as introduced, would require prior notification of a security breach be made to the OAG before the public was notified. The notification to the OAG would bring the District's law in-line with other states and gives the Attorney General the tools to take swift action when a breach occurs.²¹ It is important to note that even though notification to an Attorney General is common in other states, prior notice is only required in two other states: Maryland and New Jersey.²²

During the hearing on Bill 23-215, Chairman Phil Mendelson raised concerns that prior notification to the OAG could delay notification to a resident whose personal information was compromised. He also questioned the need to delay notification due to an ongoing law enforcement investigation as required under current law.²³ Chairman Mendelson believed that notice to a consumer must be immediate.

determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.”

¹⁶ See D.C. Official Code § 28-3851(1), which provides a good faith acquisition of data of protection information by employees or agents of the person or entity, and acquisition of data that has been rendered secured so as to be unusable by an unauthorized third party shall not be considered a breach of the security of the system.

¹⁷ See D.C. Official Code § 28-3852(a).

¹⁸ See *Supra* note 3 at 5.

¹⁹ *Supra* note 12.

²⁰ See Cal. Civ. Code § 1798.82.

²¹ See *Supra* note 3 at 5.

²² See Kyle R. Innes, Assistant Vice President & Assistant General Counsel, Securities Industry and Financial Markets Association, Written Statement Submitted to the DC Council Committee of the Whole, 2, November 8, 2019.

²³ See D.C. Official Code 28-3852(e).

The Committee Print for Bill 23-215 was updated to address the concerns raised by Chairman Mendelson. Now notification to a District resident and the OAG will be simultaneous. Moreover, the Committee Print includes a de minimis requirement for notification to the OAG in order align the District's law with other states. A company will be required to notify the OAG of a breach only if it affects 50 or more District residents. This will ensure that small businesses are not overly burdened by the notification requirements in the bill while still allowing the OAG to protect District residents when there has been a large-scale breach.

Security Requirements

Following cybersecurity best practices, Bill 23-215 would require companies take reasonable steps to protect a District resident's personal information from unauthorized access, use, modification, or a reasonably anticipated hazard or threat. This provision would require companies to take proactive steps to protect District residents. On many occasions a breach occurs because the company did not use best practices to secure data, and when this happens the consumer bears the price for this mistake.²⁴

The Committee Print was updated to reflect that a company that is in compliance with Title V of the Gramm-Blanch-Bliley Act (GLBA)²⁵ would be in compliance with the security requirements in Bill 23-215. This was done to address concerns that were raised by Mr. Innes from the Securities Industry and Financial Markets Association. He wrote to the Committee that the new security requirements are not more robust than what is required under the GLBA and they are not similar either, so it is unnecessary to require a company to follow both laws since the regulatory inconsistency can take away from a company's efforts to protect customers.²⁶

Credit Monitoring and Enforcement

In order to provide more protections to District residents, Bill 23-215, as introduced, would require a company to provide two years of identity theft protection to each District resident whose social security number or tax identification number was released in a breach. California was the first state to require free credit monitoring services. Since California adopted its law, the states of Delaware, Connecticut, and Massachusetts have passed similar laws.

Unlike what was proposed in Bill 23-215, no other state requires 24 months of free credit monitoring services for all companies that are subject to the states data breach law.²⁷ The Committee believes that this is a necessary provision to incentivize companies to be good stewards of an individual's personal information, but the credit monitoring requirement should align with other states. California, Delaware, and Connecticut require 12 months of free credit monitoring services, and Massachusetts requires 18 months of free credit monitoring.²⁸

²⁴ See *Supra* note 5 at 3.

²⁵ 15 U.S.C. § 6801 *et seq.*

²⁶ *Supra* note 22.

²⁷ Of note, Massachusetts does require 42 months of free credit monitoring services be offered by a consumer reporting agency that experiences a breach.

²⁸ See *Massachusetts Data Breach Changes - Coming April 11!*, JDSUPRA,

The Committee has determined only requiring 12 months of free credit monitoring services would be insufficient. This is due to the fact that sometimes bad actors hold on to data and use it some time after the original breach occurred. The Committee recommends a timeline similar to what is provided under Massachusetts law. It provides enough time for consumers to get the protection they need, but also would not create a substantial burden for a small business. The Committee Print of Bill 23-215 reflects this recommendation and would require all companies to provide 18 months of free credit monitoring services to a District resident.

Concerns were also raised regarding the enforcement provisions, such as the enforcement provisions in Bill 23-215 would unfairly punish businesses. However, the Committee does not agree with this assessment, and agrees with the OAG that the new enforcement provision gives real teeth in the law and creates an appropriate incentive for a company to safeguard consumers data.²⁹ These penalties should not be seen as a punishment since a company would not be subject to the penalties as long as the company is in compliance with the law. This is an incentive to be in compliance with the law.

The current penalties are some of the weakest in the country. For example, under the current law the Attorney General “may recover a civil penalty not to exceed \$100 for each violation”³⁰ The penalties for a violation of this act has not kept up, that is why the Committee agrees that the violation of the data breach law should be a violation of the District’s Consumer Protection Procedures Act (CPPA). This will increase the civil penalty to an amount that is high enough to be considered a sufficient deterrent.³¹ In addition, the bifurcated penalty system of the CPPA will allow the OAG to enact harsher penalties for recidivists.

Further, the Committee has received requests to remove the private right of action language from the law. Some believed that the private right of action provision will lead to expensive litigation and foster frivolous claims. However, the current law includes a private right of action provision and the Committee has seen no evidence of the claims that have been made.³² Moreover, removing the private right of action provision would weaken the protections for consumers.

The Committee recommends the approval of the Committee Print of Bill 23-215, because it will modernize the District’s data breach law to protect District residents. It will also update the District’s law to be modeled after others states data breach laws that have been strengthened recently.

<https://www.jdsupra.com/legalnews/massachusetts-data-breach-changes-41299/> (last visited Jan. 16, 2020).

²⁹ See *Supra* note 2 at 6.

³⁰ D.C. Official Code § 28-3853(b).

³¹ The civil penalty that the OAG can recover for CPPA violation is \$5,000 for an initial violation and \$10,000 for each subsequent violation.

³² D.C. Official Code § 28-3853(a).

II. LEGISLATIVE CHRONOLOGY

- March 21, 2019 Bill 23-215, the “Security Breach Protection Amendment Act of 2020” is introduced by Chairman Mendelson at the request of the Attorney General.
- March 29, 2019 Notice of Intent to Act on Bill 23-215 is published in the *DC Register*.
- April 2, 2019 Bill 23-215 is “read” at a Legislative meeting and the referral to the Committee of the Whole with comments from the Committee on Judiciary and Public Safety is official.
- October 25, 2019 Notice of Public Hearing on Bill 23-215 is published in the *DC Register*.
- November 1, 2019 Revised and Abbreviated Notice of Public Hearing on Bill 23-215 is published in the *DC Register*.
- November 12, 2019 The Committee of the Whole holds a public hearing on Bill 23-215.
- January 21, 2020 The Committee of the Whole marks up Bill 23-215.

III. POSITION OF THE EXECUTIVE

The Committee received no testimony or comments from the Executive on Bill 23-215.

IV. COMMENTS OF ADVISORY NEIGHBORHOOD COMMISSIONS

The Committee received no testimony or comments from Advisory Neighborhood Commissions on Bill 23-215.

V. SUMMARY OF TESTIMONY

The Committee of the Whole held a public hearing on Bill 23-215 on Tuesday, November 12, 2019. The testimony summarized below is from that hearing. Copies of written testimony are attached to this report.

Justin Brookman, Director, Consumer Privacy and Technology Policy, Consumer Reports, testified in support of Bill 23-215 because it will patch significant weaknesses in the District’s existing data breach laws. Mr. Brookman testified that this is common-sense legislation to protect consumers’ privacy and financial security. He recommended the following changes: (1) expand the bill to provide protections for all online accounts not just email accounts; (2) expand the data security requirement to cover certain data that may not trigger consumer notification; and (3) expand the definition of medical information to include dental information so there is no

loophole for oral care providers. Finally, Mr. Brookman testified that while expanding data security and breach notification requirements is real progress for consumers, this bill does not limit how companies obtain, share, and retain data in the first place, and he urged the Council to take up data privacy legislation.

Brian Young, Public Policy Manager, National Consumers League, testified in support of Bill 23-215. Mr. Young testified that Bill 23-215 would help better safeguard the data security of District residents. He added that while this bill does not address issues like how businesses obtain and share data, Bill 23-215 will take meaningful steps to compel businesses to responsibly handle District residents' data. Further, he testified that the bill provides meaningful disclosures and educational materials that consumers need to avoid fraud.

Elaine Critides, Counsel, State Privacy & Security Coalition, testified in opposition to Bill 23-215 as introduced. She testified that the Coalition supports efforts by states to update their original breach notice laws, but the Council should clarify and scale back or eliminate anomalous requirements in the bill to better serve the goals of security and notice to District residents. She recommended the following changes: (1) provide more clarity with regards to what data triggers notification requirements; (2) remove several notice content elements in the bill that are needlessly confusing; (3) clarify when service providers must provide notice; (4) require notification only if there is some risk of harm to District residents; (5) remove the proposed rulemaking authority of the Office of Attorney General; (6) give sole enforcement authority to the Office of the Attorney General by removing the private right of action provision in the current law; and (7) require the District's data breach law to apply to District government agencies.

Elizabeth Wilkins, Senior Counsel for Policy, Office of the Attorney General, testified on behalf of the Attorney General in support of Bill 23-215 as it will improve the District's ability to protect residents in the new data economy. Ms. Wilkins testified that the District's current data breach law is not strong enough to sufficiently protect District consumers because it has not been updated since the law was adopted in 2007. She added that this bill will allow the Office of the Attorney General to be coequal partners with fellow state attorneys general in policing national cybersecurity issues. Ms. Wilkins testified that the advances in the digital economy and other states' policies around data breaches mean that the District is behind the times. She closed her testimony by stating that Bill 23-215 is needed to modernize the District's data breach law to be able to ensure District residents protected.

Testimony Submitted for the Record

Brian Costello, Manager, State Government Relations, American Property Casualty Insurance Association (APCIA), wrote that APCIA recognizes the legislative objective of Bill 23-215, but the Association has significant concerns that the proposed amendment will harm rather than benefit consumers. He raised the following concerns: (1) the expanded definition of personal information could raise overnotification consequences; (2) prioritizing notice to the Office of Attorney General misaligns the goal of the law which should be meaningful notification to consumers; (3) the rulemaking authority for the Office of the Attorney General should be removed as it could further complicate and differentiate and already inconsistent patchwork of breach

notification laws; and (4) the private right of action provision will only create a frenzy of litigation activity.

Kyle R. Innes, Assistant Vice President & Assistant General Counsel, Securities Industry and Financial Markets Association, wrote in support of Bill 23-215 but provided some suggestions that would both strengthen consumer protections and increase the proposed bill's efficiency. In addition, he wrote the Gramm-Leach-Bliley Act compliance provision should be expanded to include the Office of the Attorney General notification provision and the new security requirement provision.

CareFirst BlueCross BlueShield, wrote that the company supports efforts to protect consumer data in the District. It recommended that Bill 23-215 be amended to provide that if a company follows the security requirements outlined in the bill the company will not be in violation of the Consumer Procedures Protection Act.

Erika Wadlington, Director of Public Policy & Programs, DC Chamber of Commerce, wrote in opposition to Bill 23-215. She wrote that information that has been aggregated, de-identified, or is publicly available should not be covered by the law, and that District agencies should be covered by the law. She added that a risk of harm provision should be included, that prior notification to the Office of the Attorney General is unnecessary, and information collected in other contexts such as employment, hiring of vendors, contractors or seasonal workforce should be excluded. In addition, Ms. Wadlington wrote that language should be added that recognizes a businesses' compliance with industry guidelines and federal law. Finally, she wrote that violations of the law that are not willful or reckless should not be penalized and that the Council should remove the private right of action provision from the law.

VI. IMPACT ON EXISTING LAW

Bill 23-215 amends § 28-3801 to clarify that the provisions of Subchapter 1 of Chapter 38 only apply to that Subchapter and not to all of Chapter 38.

Bill 23-215 amends the table of contents of Subchapter 2 of Chapter 38 of Title 28 to add three new section designations.

Bill 23-215 amends § 28-3851 to update the definition of a breach of the security system, and to include a new risk of harm trigger. In addition, the bill expands the definition of personal information, and adds new definitions for the term's: genetic information, medical information, and person or entity.

Bill 23-215 amends § 28-3852 to specify the required contents of a notification of a security breach. Further, the bill requires notification to the Office of the Attorney General if the security breach 50 or more District residents and provides for the required contents of the notification to the Office of the Attorney General.

Bill 23-215 adds a new § 28-3852a to specify the security requirements for protection of personal information.

Bill 23-215 adds a new § 28-3852b to require a person or entity to offer 18 months of identity theft protection services to each District resident whose social security number or tax identification number was released as a result of the security breach.

Bill 23-215 adds a new § 28-3852c to allow the Attorney General to promulgate rules to implement the notification provisions pursuant to § 28-3852.

Bill 23-215 amends § 28-3853 to make it a violation of the requirements for protection of personal information an unfair or deceptive trade practice.

Bill 23-215 amends § 28-3904 to provide that a violation of Subchapter 2 of Chapter 38 of Title 28 is an unfair or deceptive trade practice.

Bill 23-215 amends § 28-3909 to clarify the enforcement actions the Attorney General can bring against a person or entity for violations of sections § 28-3851, 28-3852, 28-3852a, and 28-3852b.

VII. FISCAL IMPACT

The attached January XX, 2020 fiscal impact statement from the District's Chief Financial Officer states that funds are sufficient in the FY 2020 through FY 2023 budget and financial plan to implement Bill 23-215.

VIII. SECTION-BY-SECTION ANALYSIS

Section 1 States the short title of Bill 23-215.

Section 2 Amends Chapter 38 of Title 28 of the District of Columbia Code.

subsection (a) makes a technical and clarifying amendment to provide that the provisions of Subchapter 1 do not apply to all of Chapter 38.

subsection (b) updates the table of contents for Subchapter 2 of Chapter 38 of Title 28 by adding three new section designations: section 28-3852a. Security Requirements; section 28-3852b. Remedies; and section 28-3852c. Rulemaking.

subsection (c) amends section 28-3851 to make updates to several definitions.

paragraph (1) clarifies that it is not a breach of the security of the system unless the information obtained has the potential to compromise the effectiveness of the security protection system. And that it is not a breach of the security of the system

if the acquisition of personal information is deemed by the person or entity, after consultation with District and federal law enforcement agencies, that the breach will likely not result in harm to the District resident.

paragraph (2) adds new definitions for the term's: genetic information and medical information.

paragraph (3) makes a conforming and technical amendment.

paragraph (4) adds a new definition for the term person or entity.

paragraph (5) expands and updates the definition of personal information to include additional information, including a person's passport number, taxpayer identification number, military ID number, health information, biometric data, genetic information and DNA profiles, and health insurance information.

subsection (d) amends section 28-3852 to update the notification requirements for a security breach.

paragraph (1) expands the notification requirements under current law by providing specific requirements for the content of that notification to consumers. Further, it allows for an alternative notification to a person if the security breach only involves an individual's email account.

paragraph (2) requires notification to the Office of the Attorney General if the security breach affects 50 or more District residents. The notice must be made in the most expedient manner possible. In addition, it provides the requirements that must be included in the notification provided to the Office of the Attorney General.

paragraph (3) requires a person or entity that is in compliance with the notification requirements of this Act due to the person or entity maintaining its own notification procedures as part of an information security policy or maintaining a procedure for a breach notification system under Title V of the Gramm-Leach-Bliley Act to provide written notification to the Official of Attorney General if a security breach that affects 50 or more District residents.

subsection (e) adds new sections 28-3852a, 28-3852b, and 28-3852c. Section 28-3852a requires a person or entity to implement and maintain reasonable safety security safeguards practices to protect the personal information of District residents. In addition, it provides that a person or entity who is in compliance with the security procedures and practices contained in Title V of the Gramm-Leach-Bliley Act shall be deemed in compliance with section 28-3852a. Section 28-3852b requires a person or entity to provide 18 months of identity theft prevention services to an individual when the breach results in the release of the individual's social security or tax identification number. Section 28-3852c provides that the Attorney General may promulgate rules to implement the

notification provisions of this Act.

subsection (f) makes a conforming amendment to the private right of action provision in the Act. In addition, it provides that a violation of this Act is a violation of the District's Consumer Protection Procedures Act.

subsection (g) makes a conforming amendment to the District's Consumer Protection Procedures Act to provide that the violation of the requirements for protection of personal information is an unfair or deceptive trade practice.

subsection (h) makes a confirming amendment to the District's Consumer Protection Procedures Act to provide the Attorney General with the authority to bring an enforcement action a person or entity for violations of sections § 28-3851, 28-3852, 28-3852a, and 28-3852b of this Act.

Section 3 Adopts the Fiscal Impact Statement.

Section 4 Establishes the effective date (standard 30-day congressional review language).

IX. COMMITTEE ACTION

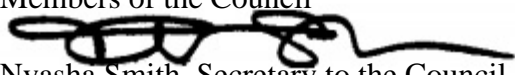
X. ATTACHMENTS

1. Bill 23-215 as introduced.
2. Written Testimony.
3. Fiscal Impact Statement for Bill 23-215.
4. Legal Sufficiency Determination for Bill 23-215.
5. Comparative Print for Bill 23-215.
6. Committee Print for Bill 23-215.

COUNCIL OF THE DISTRICT OF COLUMBIA
1350 Pennsylvania Avenue, N.W.
Washington D.C. 20004

Memorandum

To : Members of the Council

From : 
Nyasha Smith, Secretary to the Council

Date : March 25, 2019

Subject : Referral of Proposed Legislation

Notice is given that the attached proposed legislation was introduced in the Office of the Secretary on Thursday, March 21, 2019. Copies are available in Room 10, the Legislative Services Division.

TITLE: "Security Breach Protection Amendment Act of 2019", B23-0215

INTRODUCED BY: Chairman Mendelson at the request of the Attorney General

The Chairman is referring this legislation to the Committee of the Whole with comments from the Committee on Judiciary and Public Safety.

Attachment

cc: General Counsel
Budget Director
Legislative Services

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Attorney General

2019 MAR 21 PM 3:31

ATTORNEY GENERAL
KARL A. RACINE



OFFICE OF THE
SECRETARY

March 21, 2019

The Honorable Phil Mendelson
Chairman, Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, N.W.
Suite 504
Washington, DC 20004

Dear Chairman Mendelson:

I am writing to transmit the "Security Breach Protection Amendment Act of 2019". The bill amends Title 28, Chapter 38, Subchapter II of the D.C. Official Code to strengthen the protections for personal information released to unauthorized people because of the breach of the security of a computer system. The bill aims to specify the required contents of a notification of a security breach to a person whose personal information is included in a breach, to clarify timeframes for reporting breaches, to require that written notice of the breach, including specific information, be given to the Office of the Attorney General, to specify the security requirements for the protection of personal information, to make violation of the requirements for protection of personal information an unlawful trade practice, and to require the provision of 2 years of identity theft prevention services when the breach results in the release of social security or tax identification numbers. The bill makes violation of the subchapter a violation of the subchapter an unlawful trade practice subject to the remedies contained in D.C. Official Code § 28-3909.

Specifically, the bill:

- (1) Updates the definition of personal information to include additional information, including passport number, taxpayer identification number, military ID number, health information, biometric data, genetic information and DNA profiles, and health insurance information;
- (2) Inserts requirements for the content of the notification to consumers when there has been a breach, including a requirement that the notification include a statement informing residents of the right to obtain a security freeze at no cost (pursuant to federal law) and information how a resident may request a security freeze, and where appropriate the right to ID theft prevention services as described below;
- (3) Requires notification to the Attorney General;

The Honorable Phil Mendelson

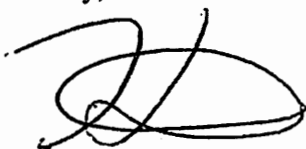
March 21, 2019

Page 2


- (4) Requires persons and entities that own, license, maintain, license, or otherwise possess personal information to implement and maintain reasonable security procedures and practices;
- (5) Adds a requirement that in the case of a breach of SSN, the company must provide 2 years of identity theft prevention services, and
- (6) Makes a violation of the data breach law a violation of the CPPA.

If you have any questions, your staff may contact my Legislative Director, James A. Pittman, on (202) 724-6517.

Sincerely,

A handwritten signature in black ink, appearing to be 'Karl A. Racine', written in a cursive style.

Karl A. Racine
Attorney General for the District of Columbia


Chairman Phil Mendelson
at the request of the Mayor

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To amend Title 28 of the District of Columbia Official Code concerning businesses' data breaches to expand definitions, to specify the required contents of a notification of a security breach to a person whose personal information is included in a breach, to clarify timeframes for reporting breaches, to require that written notice of the breach, including specific information, be given to the Office of the Attorney General, to specify the security requirements for the protection of personal information, to make violation of the requirements for protection of personal information an unlawful trade practice, and to require the provision of 2 years of identity theft prevention services when the breach results in the release of social security or tax identification numbers.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Security Breach Protection Amendment Act of 2019".

Sec. 2. Title 28, Chapter 38 of the District of Columbia Official Code is amended as follows:

(a) Section 28-3801 is amended by striking the "chapter" and inserting the word "subchapter" in its place.

(b) The table of contents for subchapter II is amended by adding three new section designations to read as follows:

"§ 28-3852a. Security Requirements.

30 “§ 28-3852b. Remedies.”.

31 “§ 28-3852c. Rulemaking.”.

32 (c) Section 28-3851 is amended as follows:

33 (1) Paragraph (1) is amended by striking the phrase “shall not be deemed to be a
34 breach of the security of the system” and inserting the phrase “shall not be deemed to be a breach
35 of the security of the system unless any information obtained has the potential to compromise the
36 effectiveness of the security protection preventing unauthorized access” in its place.

37 (2) New paragraphs (1A) and (1B) are added to read as follows:

38 “(1A) Genetic information has the meaning ascribed to it under the federal Health
39 Insurance Portability and Accountability Act of 1996 (“HIPAA”), approved August 21, 1996
40 (Pub. Law 104-191; 110 Stat. 1936), as specified in 45 C.F.R. § 106.103.

41 “(1B) Medical Information means any information about a consumer’s medical or
42 mental health treatment or diagnosis by a health care professional.”.

43 (3) Paragraph (3) is amended to read as follows:

44 “(3)(A) "Personal information" means:

45 “(i) An individual's first name, first initial and last name, or any
46 other personal identifier, which, on its own or in combination with any of the following data
47 elements, can be used to identify a person or the person’s information:

48 “(I) Social security number, Individual Taxpayer
49 Identification Number, passport number, driver’s license number, military identification number,
50 or other identifier issued by the District of Columbia or any local, state or federal government
51 agency;

52 “(II) Account number, credit card number or debit card
53 number, or any other number or code or combination of numbers or codes, such as an
54 identification number, account number, security code, access code, or password, that allows
55 access to or use of an individual's financial or credit account;

56 “(III) Medical information;

57 “(IV) Genetic information and deoxyribonucleic acid
58 profile;

59 “(V) Health insurance information, including a policy
60 number, subscriber information number, or any unique identifier used by a health insurer to
61 identify the person that permits access to an individual's health and billing information;

62 “(VI) Biometric data of an individual generated by
63 automatic measurements of an individual's biological characteristics such as a fingerprint, voice
64 print, genetic print, retina or iris image, or other unique biological characteristic, that can be used
65 to uniquely authenticate the individual's identity when the individual accesses a system or
66 account; or

67 “(VII) Any combination of data elements included in sub-
68 sub-sub paragraphs (I) through (VI) of this sub-subparagraph that would be sufficient to permit a
69 person to commit or attempt to commit identity theft without reference to a person's first name
70 or first initial and last name or other independent personal identifier.

71 “(ii) A user name or e-mail address in combination with a
72 password, security question and answer or other means of authentication, or any combination of
73 data elements included in sub-sub-sub paragraphs (I) through (VI) that permits access to an
74 individual's e-mail account.”.

75 (d) Section 28-3852 is amended as follows:

76 (1) A new subsection (a-1) is added to read as follows:

77 “(a-1) The notification required under subsection (a) of this section shall include:

78 “(1) To the extent possible, a description of the categories of information that
79 were, or are reasonably believed to have been, acquired by an unauthorized person, including the
80 elements of personal information that were, or are reasonably believed to have been, acquired;

81 “(2) Contact information for the person or entity making the notification,
82 including the business address, telephone number, and toll-free telephone number if one is
83 maintained;

84 “(3) The toll-free telephone numbers and addresses for the major consumer
85 reporting agencies, including a statement notifying the resident of the right to obtain a security
86 freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may
87 request a security freeze; and

88 “(4) The toll-free telephone numbers, addresses, and website addresses for the
89 following entities, including a statement that an individual can obtain information from these
90 sources about steps to take to avoid identity theft:

91 “(A) The Federal Trade Commission; and

92 “(B) The Office of the Attorney General for the District of Columbia.

93 “(5) Information regarding identity theft protection where when required under
94 28-3852b.”.

95 (2) New subsections (b-1) and (b-2) are added to read as follows:

96 “(b-1) Prior to giving the notification required under subsection (a) of this section, and
97 subject to subsection (d) of this section, the person or entity required to give notice shall provide

98 written notice of the breach of the security system to the Office of the Attorney General. This
99 notice shall include:

100 “(1) The name and contact information of the person or entity reporting the
101 breach;

102 “(2) The name and contact information of the person or entity that experienced
103 the breach;

104 “(3) The nature of the breach of the security of the system, including the name of
105 the person or entity that experienced the breach;

106 “(4) The types of personal information compromised by the breach;

107 “(5) The number of District residents affected by the breach;

108 “(6) The cause of the breach, including the person responsible for the breach, if
109 known;

110 “(7) Any remedial action taken by the person or entity;

111 “(8) The date and time frame of the breach, if known; and

112 “(9) A sample of the notice to be provided to District residents.

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

116 (3) Subsection (e) is amended by inserting the following sentence at the end: “The
117 person or entity shall, in all cases, provide written notice of the breach of the security of the
118 system to the Office of the Attorney General as required under subsection (b-1) of this section.”
119 in its place.

120 (4) Subsection (g) is amended by striking the phrase “with this section” and
121 inserting the phrase “with this section with respect to the notification of residents whose personal
122 information is included in the breach. The person or entity shall, in all cases, provide written
123 notice of the breach of the security of the system to the Office of the Attorney General as
124 required under subsection (b-1) of this section” in its place.

125 (e) New sections 28-3852a, 28-3852b, and 28-3852c are added to read as follows:

126 “§ 28-3852a. Security requirements.

127 “(a) To protect personal information from unauthorized access, use, modification,
128 disclosure or a reasonably anticipated hazard or threat, a person or entity that owns, licenses,
129 maintains, handles or otherwise possesses personal information of an individual residing in the
130 District shall implement and maintain reasonable security safeguards, including procedures and
131 practices, that are appropriate to the nature of the personal information and the nature and size of
132 the entity or operation.

133 “(b) A person or entity that uses a nonaffiliated third party as a service provider to
134 perform services for a person or entity and discloses personal information about an individual
135 residing in the District under a written agreement with the third party shall require by the
136 agreement that the third party implement and maintain reasonable security procedures and
137 practices that:

138 “(1) Are appropriate to the nature of the personal information disclosed to the
139 nonaffiliated third party; and

140 “(2) Are reasonably designed to protect the personal information from
141 unauthorized access, use, modification, disclosure.

142 “(c) When a person or entity is destroying records, including computerized or electronic
143 records and devices containing computerized or electronic records, that contain personal
144 information of a consumer, employee, or former employee of the person or entity, the person or
145 entity shall take reasonable steps to protect against unauthorized access to or use of the personal
146 information, taking into account:

147 “(1) The sensitivity of the records;

148 “(2) The nature and size of the business and its operations;

149 “(3) The costs and benefits of different destruction and sanitation methods; and

150 “(4) Available technology.”.

151 “§ 28-3852b. Remedies

152 “When a person or entity experiences a breach of the security of the system that requires
153 notification under subsection § 28-3852(a) or (b), and such breach includes or is reasonably
154 believed to include a social security number or taxpayer identification number, the person or
155 entity shall offer to each District resident whose social security number or tax identification
156 number was released identity theft protection services at no cost to such District resident for a
157 period of not less than 24 months. The person or entity that experienced the breach of the
158 security of its system shall provide all information necessary for District residents to enroll in the
159 services required under this subsection. This section shall not apply to an action of an agency of
160 government.”.

161 “§ 28-3852c. Rulemaking

162 The Attorney General for the District of Columbia, pursuant to § 2-501 et seq. may issue
163 rules to implement the provisions of this subchapter.”.

164 (f) Section 28-3853(b) is amended to read as follows:

165 “(b) A violation of this subchapter, or any rule issued pursuant to the authority of this
166 subchapter, is an unlawful trade practice within the meaning of Chapter 39 of this Title and is
167 subject to the remedies contained in § 28-3909.”.

168 Sec. 3. Fiscal impact statement.

169 The Council adopts the fiscal impact statement of the Chief Financial Officer as the fiscal
170 impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act,
171 approved December 24, 1973 (87 Stat. 813; D.C. Official Code §1-206.02(c)(3)).

172 Sec. 4. Effective date.

173 This act shall take effect following approval by the Mayor (or in the event of veto by the
174 Mayor, action by the Council to override the veto), a 30-day period of congressional review as
175 provided in 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973
176 (87 Stat. 813; D.C. Official Code §1-206.02(c)(1)), and publication in the District of Columbia
177 Register.

178

179

GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL

ATTORNEY GENERAL
KARL A. RACINE



Legal Counsel Division

MEMORANDUM

TO: Alana Intrieri
Executive Director
Office of Policy and Legislative Affairs

FROM: Arthur J. Parker
Acting Deputy Attorney General
Legal Counsel Division

DATE: March 20, 2019

SUBJECT: Legal Sufficiency Certification of the "Security Breach Protection
Amendment Act of 2019"
(AL-19-255)

This is to Certify that this Office has reviewed the above-referenced bill and has found it to be legally sufficient. If you have any questions regarding this certification, please do not hesitate to contact me at 724-5565.

A handwritten signature in cursive script, appearing to read "A. Parker".

Arthur J. Parker



Statement of

Justin Brookman
Director, Consumer Privacy and Technology Policy
Consumer Reports

Before the

Council of the District of Columbia
Committee of the Whole

on

Bill 23-215, Security Breach Protection Amendment Act of 2019

November 12, 2019

John A. Wilson Building
Room 412
1350 Pennsylvania Avenue, NW
Washington, DC 20004
11:00 am

Consumer Reports¹ appreciates the opportunity to provide testimony on the need for strong data security and data breach notification requirements. Residents of the District of Columbia deserve additional protections, because consumers remain more vulnerable to data breaches than ever. Companies have dramatically expanded their data collection practices as they have found new ways to monetize consumer data, but incentives to protect consumer data from unauthorized disclosure remain inadequate. For example, The Equifax data breach of 2017 led to the disclosure of the personal information, including Social Security numbers, of over 145 million Americans—about half of the United States population—leaving them susceptible to identity thieves seeking to open credit in their names for years to come.² The breadth and depth of personal information involved could all-too readily also be used to defraud and otherwise manipulate the individuals affected.³

To that end, Consumer Reports supports Bill 23-215, the Security Breach Protection Amendment of 2019, a bill that would patch significant weaknesses in the District of Columbia's existing data breach laws. The bill expands protections over personal data by requiring businesses to implement reasonable safeguards over personal information to help prevent data breaches. It also extends existing data breach notification requirements to cover additional categories of sensitive data, including information that can be used to access an email account,

¹ Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications. It employs its rigorous research and testing, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive effective legislative and regulatory solutions and fair competitive practices. Consumer Reports works for pro-consumer policies in the areas of telecommunications and technology, financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace.

² Jeremy C. Owens, *The Equifax Data Breach, In One Chart*, MARKETWATCH (Sept. 10, 2018), <https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07>.

³ Kelli B. Grant, *Your Next Worry After the Equifax Data Breach: Fake Tax Returns*, CNBC (Oct. 9, 2017), <https://www.cnbc.com/2017/09/18/your-next-worry-after-the-equifax-breach-fake-tax-returns.html>.

passport numbers, taxpayer identification information, biometric information, DNA profiles, and medical information, so that companies are required to notify consumers if the data is breached. We urge members of the DC City Council to support this common-sense legislation to better protect consumers' privacy and financial security.

While breaches can occur even when companies take reasonable precautions, many breaches have been caused by companies' carelessness and lack of accountability. It's time for the District of Columbia to make data security a priority, and to pass a law establishing these essential consumer protections. Without a clear regulatory framework for data security, companies have insufficient incentives to be better stewards of consumers' personal data. The market simply will not fix this problem—indeed, it was not until the states began enacting data breach laws in the early 2000s that companies even disclosed their breaches to the public. Although all of the states and the District of Columbia have now passed data breach notification laws,⁴ only about half of the states have data security laws—nor is there an across-the-board federal requirement—which is needed to prevent breaches from happening in the first place.⁵ This bill fills an important gap in protections, and by passing this bill, the District of Columbia will help encourage the remaining states to follow suit.

The damage caused by data breaches is wide-ranging. Security breaches of retailers, financial institutions, data brokers, businesses, government agencies, and universities are now

⁴ See *2019 Security Breach Legislation*, NAT'L COUNCIL OF STATE LEGISLATURES (July 26, 2019), <http://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx>.

⁵ See *Data Security Laws, Private Sector*, NAT'L COUNCIL OF STATE LEGISLATURES (May 29, 2019), <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>.

commonplace. There were over 2,000 data breaches in the United States and abroad in 2018.⁶ One survey revealed that nearly one-third of United States consumers were notified of an unauthorized disclosure of their information in 2017.⁷ In what is widely considered the largest hack of personal information in history, web service provider Yahoo's 2013 data breach exposed the information of anywhere from one to three billion consumers.⁸ A data breach in 2015 of the U.S. government's Office of Personnel Management's background investigation databases exposed the sensitive data of 21.5 million individuals.⁹ And these breaches have a significant impact on consumers. Americans lost nearly \$3.4 billion to new account fraud in 2018, up from about \$3 billion the previous year.¹⁰

Data breaches are harmful for businesses—in 2018, the average cost of a breach to companies globally climbed to \$3.9 million, a 12 percent increase over the past five years.¹¹ Summit Credit Union of Madison, Wisconsin testified that fraudulent charges related to data breaches cost them hundreds of thousands of dollars in 2017, not even counting the costs to replace credit and debit cards and for staff time to help resolve issues.¹² And as Pew Research

⁶ *2019 Data Breach Investigations Report, Executive Summary*, VERIZON 2 (2019), <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf> [hereinafter Verizon Data Breach Report].

⁷ Press release, *One-Third of Consumers Notified Their Data Was Breached*, HSB (Mar. 22, 2018), <https://www.businesswire.com/news/home/20180322005652/en/One-Third-Consumers-Notified-Data-Breached>.

⁸ Dell Cameron, *The Great Data Breach Disasters of 2017*, GIZMODO (Dec. 27, 2017), <https://gizmodo.com/the-great-data-breach-disasters-of-2017-1821582178>.

⁹ *Cybersecurity Incidents*, OPM.GOV, <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>.

¹⁰ *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, JAVELIN (Mar. 6, 2019), <https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt>.

¹¹ *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years*, IBM NEWSROOM (July 23, 2019), <https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Feltfor-Years>.

¹² *Examining the Current Data Security and Data Breach Notification Regulatory Regime*, Hearing Before the House Fin. Svcs. Subcomm. on Fin. Institutions and Consumer Credit at 2 (Feb. 14, 2018) (Statement of Kim M. Sponem), available at

Center points out, these data breaches are causing consumers to lose their faith in institutions, as Americans “lack confidence in various institutions to keep their personal data safe from misuse.”¹³ Most of these breaches—43%—targeted small businesses.¹⁴

In addition to requiring security protections, this bill also takes the important step of expanding the definition of personal information. Biometric data, for example, clearly warrants additional protections. Biometric data is commonly used to confirm consumers’ identity and can easily be exploited for identity theft and fraud purposes. Unlike a credit card number, the consumer’s biometric information cannot be changed in the event of a breach, making its unauthorized disclosure all the more dangerous. But concerns about its disclosure go far beyond its potential misuse for the purposes of fraud. Aside from the inherent privacy interest in keeping this information secure, the disclosure of biometric data—for example, of voice recordings—could lead to reputational or emotional harm. In light of the plethora of data breaches in recent years, biometric data should have these additional protections.

The bill also extends protections to DNA data. There are few legal requirements on companies collecting DNA, and given the increased collection of this data through sites such as 23andMe, at the very least, companies should be required to keep it secure. Companies need these incentives to protect this data: the DNA testing service Vitagene recently revealed that it left information derived from DNA data, including gene-based health information, unsecured on

https://www.cuna.org/uploadedFiles/Advocacy/Actions/Comment_Calls,_Letters_and_Testimonies/2018/Testimonies/KimSponem_Testimony_February%2014%202018.pdf.

¹³ Aaron Smith, *Americans and Cybersecurity*, PEW RESEARCH CTR. (Jan. 26, 2017), <https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/>.

¹⁴ Verizon Data Breach Report, *supra* note 5, at 2.

a server for years.¹⁵ And in 2018, the ancestry site MyHeritage, which collects DNA data, disclosed that they left email addresses and hashed passwords unprotected on a server.¹⁶

Breaches of this type of data can have devastating consequences: thieves could demand a ransom for the data, or it could be sold to insurance companies seeking to making important decisions about consumers.¹⁷

Covering taxpayer identification numbers, as well, will help prevent tax identity theft, which occurs when thieves use consumers' identifying information to obtain tax refunds. This is a serious problem: in 2017, Americans lost an estimated \$1.6 billion to tax ID fraud.¹⁸ This bill also bridges an important gap by protecting passport information. The 2018 Marriott data breach, in which the passport information of over 5 million people was disclosed, highlights the need for greater security of government-issued identification.¹⁹ Passport information, combined with other data, can be used to impersonate consumers online, making them more vulnerable to fraud.²⁰

This bill expands protections with respect to notification by requiring companies to provide consumers with meaningful information about the information that was breached and how to respond. For consumers, notice of a data breach is necessary so that they can protect

¹⁵ Nico Grant, *DNA Test Service Exposed Thousands of Client Records Online*, BLOOMBERG (July 9, 2019), <https://www.bloomberg.com/news/articles/2019-07-09/dna-testing-service-exposed-thousands-of-customer-records-online>.

¹⁶ Makena Kelly, *MyHeritage breach leaks millions of account details*, THE VERGE (June 5, 2018), <https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach>.

¹⁷ Angela Chen, *Why a DNA data breach is much worse than a credit card leak*, THE VERGE (June 6, 2018), <https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics>.

¹⁸ Joe Davidson, *Thieves targeted \$12 billion through IRS tax fraud*, WASH. POST (Oct. 19, 2018), <https://www.washingtonpost.com/politics/2018/10/19/thieves-targeted-billion-through-irs-tax-fraud/>.
<https://www.irs.gov/newsroom/writtentestimony-of-john-a-koskinen-before-the-senate-finance-committee-on-the-2017-filing-season-and-irs-operationsapril-6-2017>.

¹⁹ Peter Holly, *Marriott: Hackers accessed more than 5 million passport numbers during November's massive data breach*, WASH. POST (Jan. 4, 2019), <https://www.washingtonpost.com/technology/2019/01/04/marriott-hackers-accessed-more-than-million-passport-numbers-during-novembers-massive-data-breach>.

²⁰ Laura Hautala, *Marriott breach: What to do when hackers steal your passport number*, CNET (Dec. 3, 2018), <https://www.cnet.com/news/marriott-breach-what-to-do-when-hackers-steal-your-passport-number/>.

themselves from identity theft or other harms. Knowing what data was exposed can guide consumers in choosing which steps, in addition to security freezes and credit monitoring, they must take to avert additional forms of identity theft, such as medical or tax fraud. Consumers consistently reported after the Equifax data breach that they were frustrated by the confusing and unhelpful information that Equifax provided to them following the incident. This bill will help ensure that consumers get the information they need to respond effectively.

The bill will also benefit consumers by requiring companies to provide free credit monitoring for two years following breaches of an SSN or taxpayer identification number. Many companies profit handsomely from using consumer data, but they offer consumers little or no recourse for data lapses. This remedy will help incentivize companies keep data secure and will offer to consumer some redress following a breach. While credit monitoring provides less protection than a credit freeze—which are now free under federal law²¹—it does provide useful and immediate information that could be used to limit the consequences of identity theft after the fact.

While this bill takes key steps to protect consumer data, it should be strengthened to help avoid any unintentional gaps in coverage. For example, while we appreciate that this bill expands protections to cover email accounts, covering all online accounts would better ensure that sensitive information that, once disclosed, could cause reputational or other harm, is covered. Further, the data security requirement should be expanded to cover certain data that may not necessarily trigger consumer notification. For example, companies should be required to keep behavioral data, search history, and shopping history secure, as it can reveal more about

²¹ U.S. Code § 1681(i).

consumers than they might want to share with others: their sexual preferences, health issues, and political activities. In addition, the bill defines medical information to be about a consumer's medical or mental health treatment or diagnosis. This could inadvertently leave out dental information, or create a loophole for oral care providers, and should be modified to explicitly include oral health treatment. Finally, there may be overlap in subsection (IV) "biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as ... genetic print: and subsection (VI) "Genetic information and deoxyribonucleic acid profile," leaving the difference between the two subject to interpretation; we suggest further refinement to clearly distinguish the two in order to avoid any unintended future interpretation. We look forward to working with the author to perfect the bill as it moves through the legislative process.

Finally, while expanding data security and breach notification requirements is real progress for consumers, this bill does not limit how companies obtain, share, and retain data in the first place. Fundamentally consumers need legislation that limits commercial collection and retention to what is reasonably necessary to provide services to consumers. Several states are considering data privacy laws in the wake of California's first-in-the-nation privacy law—the California Consumer Privacy Act (or CCPA)²²—that gives consumers the ability to delete extraneous data held by companies and opt out of the sale of their information. Previously, we supported legislation before the Council that limited internet service providers' ability to monitor and sell data about customers;²³ similar legislation was passed last year in Maine.²⁴ We strongly

²² Cal. Civ. Code § 1798.100 et seq.

²³ B22-0403 (2017).

²⁴ Maine 2019 SB 275.

urge the Council to take up data privacy legislation, and Consumer Reports would be happy to assist the Council in any way possible toward extending DC residents these protections.

Councilmembers have a unique opportunity to guarantee basic security protections with respect to consumer data. For too long, inadequate laws have allowed companies to collect and profit from the use of consumers' personal information without consumers' knowledge or control, and without the incentives to properly steward that information and protect it from criminals. Given the unprecedented level of data collection in today's marketplace, and emergence of new privacy threats every day, now is the time to ensure that DC residents have the data protections they deserve. We thank you for your work to address these vital consumer protection issues.

Testimony of

Brian Young

Public Policy Manager

of the National Consumers League

on

Bill 23-215, Security Breach Protection Amendment Act of 2019

Before the

Council of the District of Columbia

Committee of the Whole

November 12, 2019

John A. Wilson Building

Room 412

1350 Pennsylvania Avenue, NW

Washington, DC 20004

11:00 am

Chairman Mendelson and distinguished Councilmembers of the District of Columbia, the National Consumers League appreciates the opportunity to present the following testimony to the Committee of the Whole in support of The Security Breach Protection Amendment Act of 2019 and the need for the Council of the District of Columbia to take action to protect District residents from the scourge of data breaches.

Founded in 1899, the National Consumers League (NCL) is the nation's pioneering consumer organization. Headquartered here in the District, our non-profit mission is to advocate on behalf of consumers and workers in the District, the United States and abroad.¹ Through NCL's Fraud.org campaign, NCL offers free fraud counseling, and educates consumers across the country on how to protect themselves in the aftermath of data breaches.²

Sadly, there has been no shortage of data breaches. Equifax, Capital One, Yahoo!, Marriott, Anthem, JP Morgan Chase, and thousands of others have all compromised consumers personal information, putting all of us at greater risk of identity fraud and other crimes. In fact according to the Identity Theft Resource Center (ITRC), there have been around 11,000 data breaches and over 1.6 billion compromised records since 2005.³ That number appears to be growing. In the ITRC's latest report, they observed a year over year increase of 126 percent in

¹ For more information, visit www.nclnet.org.

² For more information, visit <https://www.fraud.org/>

³ Identity Theft Resource Center. "Data Breaches." 2019. Online: <https://www.idtheftcenter.org/data-breaches/>

2018 of the number of compromised records which contained sensitive identifiable information.⁴

In the aftermath of a data breach, fraudsters, scammers, and identity thieves manipulate the breach data to further harm consumers. Leaked login credentials are often used to access other accounts that use the same username and password combination. Data obtained via a breach can be used to craft more convincing phishing emails, conduct social engineering attacks on call centers, open new lines of credit and steal consumers' tax refunds, to name just a few of the harms that can stem from breaches.

DC residents are not immune to this threat. A survey conducted by Wallet Hub, a personal finance website based in the District, found that when compared to the 50 other states, the District of Columbia had the highest cases per capita of identity theft and fraud in the nation.⁵ It is for these reasons that we are strongly supportive of the Security Breach Protection Amendment Act of 2019, which would help better safeguard the data security of District residents.

First, this bill extends the definition of personal information to cover extremely sensitive data that if controlled by scammers, could wreak havoc on consumers. Without this bill, information including passport or military ID numbers; health information; biometric data

⁴ Identity Theft Resource Center. "2018 End of Year Data breach Report." January 28, 2019. Online: [ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf](#)

⁵ McCann, Adam. "2019's States Most Vulnerable to Identity Theft and Fraud." Wallet Hub. October 16, 2019. Online: <https://wallethub.com/edu/states-where-identity-theft-and-fraud-are-worst/17549/#main-findings>

such as an individual's voice or finger print or other unique biological characteristics; and DNA profile information would not receive the protection it deserves.

Second, this legislation will provide meaningful improvements to the District's breach notification standard. Under this section District residents will be notified what types of data were potentially compromised, and be given the information they need to contact the business directly as well as educational information on how they can receive a credit freeze free of charge and protect themselves from identity theft.

Third, this bill empowers the Attorney General's office to proactively help breach victims via a requirement to promptly notify the Attorney General's office of a breach.

Finally, this consumer protection bill will help stop breaches before they happen by requiring holders of personal data, to take reasonable steps to secure and safeguard the data they have been entrusted with. As technology changes, so do cybersecurity best practices. NCL appreciates the regulatory flexibility that this bill provides to ensure that businesses are encouraged to take proactive steps to secure user data. When breaches happen, it is often because the business did not utilize current best practices to secure data, and yet, it is the consumer that bears the price for the business' misstep. Consumers cannot and should not be expected to carry the load when it comes to protecting the data they share with businesses and other organizations.

As the problem of data breaches continues to grow, so does the risk to Washingtonians of falling victim to identity theft, and other types of fraud. While this bill does not address critical

issues like how businesses obtain and share data, and the control consumers need to have over this process, the Security Breach Protection Amendment Act of 2019 will take meaningful steps to compel businesses to responsibly handle District residents' data. Likewise, this bill provides meaningful disclosures and educational materials that consumers need to avoid fraud.

NCL believes that each councilmember has a unique opportunity to safeguard District residents' data, and thus urges the Council of the District of Columbia to quickly pass and implement this critical consumer protection bill.

Thank you for your time.

**STATEMENT OF ELAINE CRITIDES
COUNSEL, STATE PRIVACY & SECURITY COALITION**

**BEFORE THE DC CITY COUNCIL
COMMITTEE OF THE WHOLE**

ON

BILL 23-215, SECURITY BREACH PROTECTION AMENDMENT ACT OF 2019

November 12, 2019

**John A. Wilson Building, Room 412
1350 Pennsylvania Avenue, NW
Washington, DC 20004
11:00 am**

Chairman Mendelson and members of the Committee,

My name is Elaine Critides. I am testifying today on behalf of the State Privacy & Security Coalition, an organization of 27 companies and 6 trade associations that advocates for consistent, clear and workable requirements in state privacy, data security breach and cybersecurity laws.

All 50 states and the District of Columbia already have data breach notice laws. Our Coalition supports efforts by states to update their original breach notice laws to cover additional risky data elements, breach notice content, or adopting “reasonable security” requirements for data breach notice data elements. These existing laws provide good roadmaps about how to update data security laws.

However, it is extremely important that states and territories adopt state data breach and data security laws that are consistent with laws in other states. This is because data security and cybersecurity are complicated risk management activities that require businesses and organizations to keep up with rapidly escalating and changing attack methods. Similarly, responding to a significant data security breach involves often requires conducting or overseeing a complex forensic investigation and conducting crisis management. In these contexts, complying with outlier requirements in the District or any state hinders, instead of advancing, the interests of consumers.

For these reasons, we urge you to clarify and scale back or eliminate anomalous requirements in this bill. These changes would better serve the goals of security and notice to District residents, while updating and strengthening the District’s laws in this area. Doing so is particularly important because of the dramatic expansion of enforcement authority in the bill.

1. Clarity regarding what data triggers notification requirements

For the reasons I just described, data breach and data security laws need to be very clear as to what information and situations trigger notice obligations and what information must be secured.

While some elements of the broader definition of “personal information” make sense and are consistent with other laws, other aspects are unnecessary and overbroad. In fact, the amendments to current law put forward in this bill appear to make unauthorized acquisition of a very broad range of data that are not even identifiable a data breach.

For example, the inclusion of an “other identifier” issued by a DC agency as part of the definition of personal information is counterproductive, both because it is unclear and because it undermines efforts to deidentify or pseudonymize information. These practices are privacy protective precisely because they make it harder for unauthorized actors to use the data in a way that could harm the consumer.

Furthermore, adding to the risk of harm standard “any combination of data elements included in sub-sub-sub paragraphs (I) through (VI) of this sub-sub paragraph that would be sufficient to permit a person to commit or attempt to commit identity theft” is a vague standard found in no state breach notice law. What is more, *any information* can be used to “attempt to commit identity theft”, so this standard is potentially limitless.

2. Simplifying data breach notice content requirements

Many of the “second-generation” data breach notice laws contain notice content requirements. A handful of the states have outlier requirements, which create compliance traps for businesses and increase compliance costs by requiring hiring sophisticated law firms like the one at which I practice, but do *not* provide materially better information to residents receiving the notices.

While most of the notice content elements in the bill are consistent with other states and useful to residents, several are not or are needlessly confusing, and should be removed. These include: (1) “categories of personal information” reasonably believed to have been acquired, instead of the specific sensitive data elements that have been required, which is what residents really need to know about; (2) the street address of regulators, which is irrelevant; and (3) specific contact information for the State AG’s Office (over and above the FTC, which has superb information applicable nationwide for what to do in response to a data breach).

What is more, the bill, contrary to almost every state breach notice law, would impose the same notice content requirements for email password breaches as for breaches of driver’s license numbers. What is required in email password breaches is a different notice instructing users to change their password for their email account and other online accounts. This simple step, which is a best practice, prevents misuse of these accounts. This different notice requirement is the law in California and other states that both have prescriptive notice requirements and require notice of password breaches. It should be added to this bill to better protect residents and to avoid sending irrelevant breach notice information that would confuse state residents from taking the right steps to protect themselves.

With regard to notice to the State AG’s Office, notice should not include the “remediation information” to the extent that this is intended to cover security measures taken in response to the breach, because hackers often use this information to launch secondary attacks. Furthermore, it should not include “the cause of the breach” or “the person responsible for the breach”, as this information is often subjective and complicated and not able to be conveyed in a prompt notice.

3. Clarify when service providers must provide notice

Equally problematic is lack of clarity regarding when service providers must provide notice. Most state breach laws require notice to the owner of the data by service providers that store or maintain the “personal information” and suffer a breach. The language in DC’s breach law goes further, also requiring notice by entities that “handle” the personal data. This term is confusing and suggests that *both the entity that maintains or stores the data and other “handlers”* should provide notice. Double notice serves no purpose. The obligation should only apply to entities that maintain or otherwise possess the personal data, consistent with other state laws.

4. Adding a Risk of Harm Trigger

The overwhelming majority of state breach notice laws require notice to state residents only if there is some risk of harm (almost always risk of identity theft or fraud) to state residents. This risk criterion for breach notice would avoid de-sensitizing DC residents to notices that actually pose risk to them because they receive notices about “technical” breaches.

A classic and very common example is accidental transmission of customer information to a service provider that is trusted and has signed a confidentiality agreement with the entity that sends the information, but that is not the right entity to receive the information. This would be a notifiable data breach under the bill as introduced for a very broad range of data, but would pose no risk to any DC resident.

Over the past few years, several states – most recently New York -- that had no risk of harm trigger have amended their laws to include one. DC should do so as well, particularly because it would be significantly expanding notice requirements under this bill.

The change would *benefit* DC residents by providing notice when there is some material risk and providing information and warnings that can help residents to act. However, where there is no risk, these warnings are confusing and not useful.

5. AG Rulemaking should be removed from the law, as it introduces significant uncertainty

Almost none of the state breach notice laws contain AG rulemaking authority, because this authority is wholly unnecessary.

First, there is no reason why requirements cannot be made clear in the statute (as they are clear in other breach notice laws). Without this clarity, covered entities will face needless difficulty tracking down requirements and the requirements will be less understood and *less effective*.

Second, to the extent the council retains the “reasonable security” requirements, giving the AG’s Office unqualified rulemaking authority would introduce huge uncertainty. This authority could turn into new procurement mandates that interfere with the cybersecurity risk management for sophisticated businesses that are based upon clearly established national and international standards. Unique security requirements in the District would divert resources away from the complex task of managing these dynamic risks.

On the other hand, guidance documents for small businesses, such FTC guidance, can be helpful, but the Attorney General simply does not need any rulemaking authority, much less unqualified rulemaking authority, to produce guidance.

6. There should not be private class action enforcement of the law

It is important to understand that most businesses that suffer a data breach are themselves already a victim of crime. Making a violation of the data breach notification law an unfair trade practice — without removing the existing private right of action for consumers — unjustly punishes these companies.

It does not meaningfully protect consumers or encourage compliance because the complexity of data security means that even companies with strong practices and procedures can suffer a security incident and be forced to spend hundreds of thousands of dollars responding to lawsuits and attendant one-sided eDiscovery costs borne by defendants only.

Any amendment to the enforcement provisions of the law should give sole enforcement authority to the AG, rather than creating multiple avenues for class action lawyers to line their pockets.

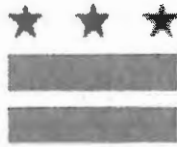
In addition, the AG penalties are up to \$10,000 per violation for any repeat violation. It is unclear whether a business' accidental failure to notify – for example, because a line employee did not report an incident contrary to a business' incident response plan – in a breach involving multiple residents would itself constitute repeat violations. For this reason, consistent with other state breach notice laws, there should be some cap on monetary penalties arising out of the same breach or series of breaches.

7. There is no principled reason to exempt DC agencies from the security or notice requirements

Government agencies typically hold far more “sensitive” information about consumers than do private sector entities in the District, and DC residents are affected equally or more when there is a breach of government “personal information.” The interests in assuring notification of DC residents in the event of a data breach are as strong or stronger in the government agency context. For this reason, we believe that all requirements and all remedies under the law should apply to all DC government agencies.

Respectfully submitted,

Elaine Critides, Counsel
State Privacy & Security Coalition
(202) 799-4501



Statement of Elizabeth Wilkins
Senior Counsel for Policy
Office of the Attorney General

Before the

The Committee of the Whole
The Honorable Phil Mendelson, Chairperson

Public Hearing

“Bill 23-215, Security Breach Protection Amendment Act of 2019”

November 12, 2019
Time 11:00am
Room 412
John A. Wilson Building
1350 Pennsylvania Avenue, NW
Washington, District of Columbia 20004

Good afternoon Chairman Mendelson, Councilmembers, staff, and residents. I am Elizabeth Wilkins, and I serve as the Senior Counsel for Policy for the Office of the Attorney General (“OAG”). I am pleased to appear on behalf of Attorney General Karl A. Racine before the Committee of the Whole to testify on OAG’s proposed bill, the Security Breach Protection Amendment Act of 2019. The bill before the Committee today makes significant advances in our ability to protect District consumers in the new data economy.

The security of consumers’ data is becoming an increasing concern in our new digital era. By consumer data, we mean any personal information that may be collected on a consumer. We used to think primarily about, say, social security numbers collected by banks. But we have seen an explosion of the breadth of information collected on people, as well as significant changes in the ways that data is collected and stored. The more data that’s out there, the more attractive it is to those who would misuse it, and the greater risk that consumers might suffer the consequences.

Our office has seen this dynamic in the frequency and increasing size of data breaches. A data breach occurs when sensitive or confidential information is intentionally or accidentally released by a company or an individual. These releases of information may happen because of insufficient security protections or as a result of hacking or cyber attacks. Recent years have seen some of the largest

and most serious data breaches in history, including the Equifax breach, which exposed the personal information of over 143 million people, including nearly 350,000 District residents.

Consumers caught in the crosshairs of these data breaches risk identity theft and other types of fraud. They may suffer financial harm, loss of significant time and resources, and even harassment.

Under our current laws, District consumers are not sufficiently protected. The District adopted our data breach laws in 2007—a lifetime ago in terms of the digital economy and cybersecurity. Many states have updated their laws to reflect these changes, and it is time the District did so as well.

After closely studying data breach laws in other jurisdictions and the latest innovations in this policy arena, our office proposed the bill at issue today, the Security Breach Protection Amendment Act of 2019. With this bill, we can protect our consumers here in the District and be coequal partners with our fellow state attorneys general in policing national cybersecurity issues.

If this bill becomes law, it would require companies that hold consumer data to do two things: maintain reasonable security procedures to safeguard consumer data, and notify consumers and the Attorney General of a breach. Certain key

reforms ensure that the law is crafted to keep up with current data practices, protect consumers, and create the right incentives:

- (1) Current law protects a narrow swath of personal information that was at issue over ten years ago when our original bill was passed. This bill updates the definition of personal information to include additional sensitive information, some of which has been the subject of recent data breaches: passport number, taxpayer identification number, military ID number, health information, biometric data, genetic information and DNA profiles, and health insurance information. This update ensures the law better protects the growing breadth of sensitive information consumers may have at risk.

- (2) Current law dictates that even where data is acquired without authorization, it does not constitute a breach if the data at issue has been rendered secure by appropriate cybersecurity techniques. The bill clarifies that a breach nevertheless *does* occur if the unauthorized access has undermined the efficacy of that security. This provision plugs a loophole to ensure that entities can be held accountable where their security measures are inadequate and consumers have been put at risk.

- (3) Current law requires that companies notify consumers of a breach. This bill inserts requirements for the content of that notification to consumers, including a requirement that it include a statement informing residents of the right to obtain a security freeze at no cost (pursuant to federal law) and, where appropriate, the right to identify theft prevention services. This increased information ensures that consumers are armed with the information they need to protect themselves.
- (4) The bill also requires notification of a breach to the Attorney General. This provision brings the District's law into line with that of most other states and ensures that OAG can take swift action in case of a breach affecting District residents.
- (5) The bill requires persons and entities that own, license, maintain, license, or otherwise possess personal information to implement and maintain reasonable security procedures and practices. This is crucial: Given the amount of data we now entrust to third parties, we must ensure that those entities treat that data with the appropriate care.

- (6) The bill adds a requirement that in the case of a breach of social security numbers, the company must provide 2 years of identity theft prevention services. Again, we want to ensure above all else that consumers are protected.

- (7) The bill makes a violation of the data breach law a violation of the Consumer Protection Procedures Act (CPPA), the District's main consumer protection statute. This provision confirms that violations of the data breach law can be addressed through enforcement under the CPPA, ensures that there are real teeth to our law, and creates the appropriate incentives for companies to safeguard the data of their consumers.

Advances in the digital economy and in other states' policies around data breaches mean that the District is behind the times. We need this modernization of our data breach law in order to ensure that District residents are protected.

Thank you for the opportunity to testify, and I am happy to answer any questions that members may have.



November 20, 2019

Re: B23-0215 – Security Breach Protection Amendment Act of 2019.

Chairman Phil Mendelson
Committee of the Whole
1350 Pennsylvania Avenue NW, Suite 410
Washington, DC 20004

Dear Chairman Mendelson,

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to provide feedback on B23-215, “Security Breach Protection Amendment Act of 2019” (B23-215). APCIA represents nearly 60 percent of the U.S. property casualty insurance market and the broadest cross-section of home, auto, and business insurers of any national trade association. Of particular interest, APCIA members represent all sizes, structures, and regions, protecting families, communities, and businesses located in the District of Columbia.

Consumer privacy and data security are a priority issue for the insurance industry and as such, insurers devote considerable resources to protect data, information systems, and consumer trust. To that end, we support policy efforts that balance corporate responsibility with appropriate oversight that ultimately enhances consumer protections. We recognize the legislative objective of B23-215 is to strengthen consumer protections related to unauthorized access to personal information because of a breach of the security of a computer system; however, APCIA has significant concerns that the amendments proposed by B23-215 will harm rather than benefit consumers. These concerns are outlined below.

Personal Information

B23-215 proposes to amend the definition of personal information to make a “personal identifier” a data element and further allows the personal identifier and individual’s first initial and last name to be considered a data element on their own. Such a broad definition would mean that an address, last name, or date of birth, for example, are independently considered personal information. These amendments raise consumer harm issues due to the overnotification consequences. APCIA respectfully urges the legislature to remove this proposed amendment. The definition of personal information in the current law appropriately strikes the right balance of notifying consumers when there is risk of a breach that presents a risk of substantial harm while avoiding the potential to desensitize consumers.

Attorney General Notice

The primary focus of a breach notification law should be meaningful notification to consumers of a material event without unreasonable delay. Prioritizing the attorney general notice misaligns these priorities. If notice to the Attorney General is necessary, the provision should be drafted to require notice

only if notice must be sent to 500 or more D.C. residents and following delivery to the consumer. This will prioritize consumer notice and the 500 resident threshold avoids inundating the Attorney General with notifications.

The proposed language permitting the Attorney General to adopt regulations should be eliminated. Allowing regulations only adds uncertainty and has the potential to further complicate and differentiate and already inconsistent patchwork of breach notification laws.

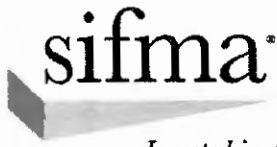
Private Right of Action

Enforcement consistent with the Consumer Protection Procedures Act (CPPA) would introduce a private right of action for violations of the breach notification and new data security requirements. The legislature should specifically exclude a private right of action. Given the Attorney General's enforcement role, a private right of action will only create a frenzy of litigation activity in an already uncertain and litigious environment.

Thank you for the opportunity to comment and if we can answer any questions, please let us know. Please contact me directly at 847-553-3732 or via email at brian.costello@apci.org or APCIA's District of Columbia counsel, Brett Greene and Tiffini Greene at 202-280-6364 or via email at tgreene@amermgmt.com.

Respectfully submitted,

Brian Costello
Manager, State Government Relations
American Property Casualty Insurance Association



Invested in America

November 8, 2019

The Honorable Phil Mendelson
Chair, Council of the District of Columbia
Chair, Committee of the Whole
Wilson Building, Room 412
1350 Pennsylvania Avenue, N.W.
Washington, DC 20004

RE: DC B23-215, A Bill Regarding Data Privacy Protection

Dear Chair Mendelson:

The Securities Industry and Financial Markets Association¹ is a national trade association which brings together the shared interests of over 340 broker-dealers, banks and asset managers, many of whom have a strong presence in the District of Columbia. We thank you for the opportunity to provide feedback on B23-215, which would generally modernize the District's data breach law while keeping the law in line with similar requirements across the country.

SIFMA generally supports such efforts and commends Attorney General Racine and the Council on their efforts in this space. Below we have included several suggestions for your review that would both strengthen consumer protections and increase the proposed framework's efficiency:

- **The Need to Expand the Gramm-Leach-Bliley Act Compliance Provision**

The current law states that entities subject to Title V of the GLBA, and who provide notice of a breach in accordance with that Act, are deemed to be compliant with the District's law. As currently drafted, B23-215 would add two new provisions to the existing law, both of which would be outside of the GLBA deemed-compliance provision: notification to the District Attorney General, and an additional security requirement. We urge you to consider expanding the GLBA deemed-compliance provision to include both provisions, or at least modifying the notification provision, for the reasons discussed below.

Public Records Requests

The proposed AG notification provision includes requirements that the cause or nature of the breach and the identity of the responsible individual be reported. Our membership has expressed significant concern that this information could be made public through a public records request, which could cause significant additional security issues. Generally, disclosing the nature or cause of a breach could reasonably lead to the inadvertent disclosure of critical system and/or security information – which

¹ SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. For more information, visit <http://www.sifma.org>.

would only be made worse if that information could also be made public. Such a disclosure could put the personal information of people in D.C. and across the country at greater risk. Similarly, reporting the name of the individual who is responsible for a breach, if known, is problematic because it could be difficult to identify a single responsible person. Additionally, the need to identify a person(s) responsible may impact an organization's decision as to how – or even if – to report, which would defeat the intent of the proposal. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to either remove these requirements (in subsections 3 and 6), or at least ensure that such reports are exempt from public records requests.

Timing of Notification

B23-215 currently requires that the D.C. Attorney General be notified prior to notifying an impacted resident of the breached information.² Several of our members are concerned that this requirement could unnecessarily delay an organization's response time. Data breach laws are most often designed to notify impacted customers of the breach so that they can take steps to protect themselves. The requirement to notify the AG first could delay the impacted customer notification, leaving them unable to take those protective measures. We believe that this is currently happening in both New Jersey and Maryland – the only two states we're aware of with a prior notification requirement. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to consider simultaneous reporting.

On a separate but similar issue, there is no timing guidance included for entities that are required to provide consumer notices. We believe a general timing requirement would be helpful (e.g., "within a reasonable time after discovery and confirmation of a breach") but believe that any set timeframe of at least 45 days after discovery and confirmation of a breach would be beneficial.

De Minimis Requirement

Currently, this bill would require notification to the AG if certain information of any single D.C. resident was breached. This would be a fairly unique requirement that could lead to unnecessary reporting and additional burdens on both reporting entities and the District AG's Office. In other states that have a single resident requirement, the state agency notification is usually included in the deemed-compliance provision. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to consider the addition of a de minimis requirement.³

Security Requirement

New Section 28-3852a would not require a greater level of security than what is already required by GLBA, but neither does it include identical requirements. Such regulatory inconsistency can take away from firm efforts to protect their customers. In fact, Firm cybersecurity staff are currently spending 40% of their time, on average, on regulatory compliance efforts, taking their time away from other cyber defense activities.⁴ As such, we strongly suggest that the GLBA deemed-compliance provision be extended to include new Section 28-3852a's security requirements.

² Please note that clarification on the numbering of the sections may prove helpful; the proposed number (b-1) and (b-2) makes them appear to be part of the requirement to notify the owner or licensee of a breach, rather than the requirement to notify consumers.

³ 500 or 1,000 residents are the two most common requirements.

⁴ Financial Services Sector Coordinating Council, "Financial Services Sector Cybersecurity Recommendations," available at: [fssc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf](https://www.fssc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf).

- **The Definition of Personal Information Should Not Include “Attempt to Commit” Language**

B23-215 currently includes any subset of information that would be sufficient for a person to “commit or attempt to commit identify theft [...]” in subsection VII of the definition of “Personal Information.” In this case, the “attempt to commit” language is both unnecessary and problematic. The entire subsection is already conditional (i.e., the definition includes information that “would be sufficient to commit [...]”) and would encompass the breach of any information which could cause harm to a consumer. On top of this, anyone could technically attempt to commit identity theft with any combination of information – regardless of whether such an attempt could ever be successful.

We appreciate your willingness to consider our suggestions. If there is any additional information we may be able to provide or any questions we can answer, please contact me at 212-313-1211 or kinnes@sifma.org with any questions.

Sincerely,

/s/

Kyle R. Innes

Assistant Vice President & Assistant General Counsel
SIFMA

CC: All Members, Committee of the Whole



**Testimony for the Record
Council of the District of Columbia
Committee of the Whole
Bill 23-0215, “Security Breach Protection Amendment Act of 2019”**

Chairman Mendelson and members of the Committee of the Whole, CareFirst BlueCross BlueShield (CareFirst) appreciates the opportunity to submit testimony for the record on Bill 23-0215, the “Security Breach Protection Amendment Act of 2019.”

Bill 23-0215 seeks to provide protections to consumers if personal information is released to unauthorized individuals due to data security breach. Importantly, the bill creates security requirements for the protection of personal information and makes violations of the legislation a violation of the District’s Consumer Protection Procedures Act (CPPA). However, the legislation makes any breach a violation of the CPPA, even if the business followed the security requirements outlined in 38-2852a.

CareFirst believes that the legislation should be amended such that if a company follows the security requirements outlined in 38-2852a they will not be in violation of the CPPA. The bill is intended to outline reasonable security procedures, and businesses should be able to rely on compliance with those procedures as sufficient to provide reasonable protections to consumers. CareFirst suggests the addition of the following at the end of line 167 of the legislation to achieve this:

“except if the company has complied with security requirements in 3852a, in which case the company will not be considered to be in violation of 28-3909.”

CareFirst supports efforts to protect consumer data in the District of Columbia.



DC Chamber of Commerce Testimony Submitted for the Public Record
To
The Committee of the Whole
on
Bill 23-215, the Security Breach Protection Amendment Act of 2019
Tuesday, November 12, 2019

The D.C. Chamber of Commerce respectfully submits this statement for the record regarding ***Bill 23-215, The Security Breach Protection Amendment Act of 2019***. The DC Chamber does not support the bill as introduced and invites your attention to provisions that we have identified with concerns as well as ways in which the proposal currently before you can be improved.

The D.C. Chamber of Commerce represents businesses large and small throughout the District of Columbia and region. At the D.C. Chamber, we work hard to make living, working, playing, and doing business in D.C. a much better proposition for all. And we, at the Chamber, support ensuring that as technology and DC's place as a data-science and information hub evolves, effective practices are in place to protect consumers. Regrettably, however, as drafted Bill 23-215 is not the vehicle to ensure that important goal is met.

1. **Definitions & Scope Should Be Reconsidered.** We agree that the definitions should be comprehensive. However, information that has been aggregated, de-identified, or is publicly available should not be covered by the law. Any personal data altered from its original form or that is encrypted should be exempted from the notification requirements. This will incentivize entities to ensure data is protected via industry-standard methods while making it harder for hackers to decipher personal information.

Should the Council consider acting on this legislation, District agencies should be covered by the act to the same extent as private companies. Those agencies likely hold as much, if not more, sensitive information than private companies operating in the District. The District's interest in keeping its residents' data secure and assuring notification of covered breaches to those residents is just as strong whether the breach affects a government agency or a private company.

As to the notification requirements, reporting and notice should not be triggered when events are merely theoretical, technical, or minimal. Additionally, the key terms should also detail a harm threshold. In approximately 40 jurisdictions throughout the United States and even some other countries, notification of a data breach is triggered only when there is a likelihood of significant harm to affected individuals or harm has occurred. Approximately half also specify a threshold number of affected residents. We ask that the Committee consider incorporating those thresholds to align with best practices and focus the notification on meaningful responses and solutions.

As to the proposed prior notice to the Attorney General, only three states currently require Attorney General notice prior to consumer notice. Whereas prompt notice to affected consumers allows them to take appropriate measures to protect themselves from identity theft, there is no purpose served by advance, potentially premature, notice to the Attorney General.

Finally, information collected in other contexts such as employment, hiring of vendors, contractors or seasonal workforce should be excluded.

Without such changes to the bill, we cannot be supportive.

- 2. Changes to Enforcement Provisions & Applicability to other Laws**– As a result of enhanced industry standards and federal laws, businesses are already taking steps and implementing policies to ensure consumer data is properly secured and protected. With the passage of data protection, privacy, or consumer protection laws like HIPPA Privacy Security and Breach Law and Gramm-Leach-Bliley Act privacy laws already apply to large sectors of our economy. Should the committee move forward with the bill we ask that language is added that would recognize that compliance with industry guidelines and federal laws would constitute compliance with the act to avoid the need for inconsistent company policies and procedures in the District. Such language would align the bill to the Children’s Online Privacy Protection Act (COPPA).

After reviewing the legislation, the concern of our membership is that this bill would place a burden on small businesses including startups and CBE vendors. For most startups, capital is limited, Now, with this already, limited capital, they will not only have to implement specific systems, fulfill the administrative compliance with the act but also would be fiscally liable for breaches when they are the injured party of the attacks. We ask that violations of the act that is neither willful nor reckless should not be penalized. After all, in many cases, it is the business entity that is the victim of the attack.

We strongly advise the Council to remove the private right of action from the law. Such provisions undermine existing enforcement capabilities, lead to expensive litigation, and foster frivolous claims.

At the DC Chamber, we are dedicated to ensuring that our city continues to grow and prosper together and that mission includes the promotion of responsible corporate practices. However, such a mission cannot be fulfilled without the partnership and inclusion of the public sector and policymakers. Thank you for the opportunity to comment on Bill 23-215. The DC Chamber looks forward to working with you to find optimal solutions to the challenges facing our city. Should you or your staff have questions or need additional information, please contact Ms. Erika Wadlington, Director of Public Policy & Programs at ewadlington@dcchamber.org or at (202) 347-7201.

**Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print**

**An Act to amend certain provisions of subtitle II of title 28, District of Columbia Code,
relating to interest and usury.
(D.C. OFFICIAL CODE § 28-3801)**

§ 28–3801. Scope — Limitation on agreements and practices.

This subchapter applies to actions to enforce rights arising from a consumer credit sale or a direct installment loan.

**Consumer Personal Information Security Breach Notification Act
(D.C. OFFICIAL CODE § 28-3851 *ET SEQ.*)**

§ 28–3851. Definitions.

For purposes of this subchapter, the term:

“(1)(A) “Breach of the security of the system” means 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.

“(B) The term “breach of the security of the system” does not include:

“(i) A good faith acquisition of personal information by an employee or agency of the person or entity for the purposes of the person or entity if the personal information is not used improperly or subject to further unauthorized disclosure;

“(ii) Acquisition of data that has been rendered secure so as to be unusable by an unauthorized third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorized access; or

“(iii) Acquisition of personal information of an individual that the person or entity reasonably determines, after consultation with District and federal law enforcement agencies, will likely not result in harm to the individual.

~~(1) “Breach of the security of the system” means 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 business. The term “breach of the security system” shall not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure. 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.~~

**Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print**

(1A) Genetic information has the meaning ascribed to it under the federal Health Insurance Portability and Accountability Act of 1996 (“HIPPA”), approved August 21, 1996 (Pub. Law 104-191; 110 Stat. 1936), as specified in 45 C.F.R. § 106.103.

(1B) Medical information means any substantive information about a consumer’s dental, medical or mental health treatment or diagnosis by a health care professional.

(2) “Notify” or “notification” means providing information through any of the following methods:

(A) Written notice;

(B) Electronic notice, if the customer has consented to receipt of electronic notice consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act, approved June 30, 2000 (114 Stat. 641; 15 U.S.C. § 7001); or

(C)(i) Substitute notice, if the person or ~~entity business~~ demonstrates that the cost of providing notice to persons subject to this subchapter would exceed \$50,000, that the number of persons to receive notice under this subchapter exceeds 100,000, or that the person or ~~entity business~~ does not have sufficient contact information.

(ii) Substitute notice shall consist of all of the following:

(I) E-mail notice when the person or ~~entity business~~ has an e-mail address for the subject persons;

(II) Conspicuous posting of the notice on the website page of the person or ~~business entity~~ if the person or ~~entity business~~ maintains one; and

(III) Notice to major local and, if applicable, national media.

(2A) “Person or entity” means an individual, firm, corporation, partnership, company, cooperative, association, trust, or any other organization, legal entity, or group of individuals. The term “person or entity” shall not include the District of Columbia government or any of its agencies or instrumentalities.

(3)(A) “Personal information” means:

(i) An individual’s first name, ~~or~~ 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: or phone number, or address, and any one or more of the following data elements:

Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print

_____ (I) Social security number, Individual Taxpayer Identification Number, passport number, driver’s license number, military identification number, or other identifier issued by the District of Columbia or any local, state or federal government agency;

_____ (II) Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual’s financial or credit account;

~~Driver’s license number or District of Columbia Identification Card number; or~~

_____ (III) Medical Information~~Credit card number or debit card number;~~

_____ (IV) Genetic information and deoxyribonucleic acid profile;

_____ (V) 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;

_____ (VI) 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 can be used to uniquely authenticate the individual’s identity when the individual accesses a system or account; or

_____ (VII) Any combination of data elements included in sub-sub-sub paragraph (I) through (VI) of this sub-paragraph that would enable a person to commit identity theft without reference to a person’s first name or first initial or other independent personal identifier.

~~(ii) 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 sub-sub-sub paragraphs (I) through (VI) that permits access to an individual’s email account. Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual’s financial or credit account.~~

(B) For purposes of this paragraph, the term “personal information” shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

§ 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

Bill 23-215, "Security Breach Protection Amendment Act of 2020"
Committee of the Whole
Draft Comparative Print

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.

(5) Information regarding identity theft protection where when required under 28-3852b.

"(a-2) Notwithstanding subsection (a-1), in the case of a breach of the security of the system that only involves personal information defined in section 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 notification required under subsection (a) of this section, the person or entity required to give notice shall promptly provide written notice of the breach of the security

Bill 23-215, "Security Breach Protection Amendment Act of 2020"
Committee of the Whole
Draft Comparative Print

of the system to the Office of the Attorney General if the breach affects 50 or more District residents. This notice shall be made in the most expedient manner possible, without unreasonable delay, and no later than when notice is required by 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 system;
- (4) The types of personal information compromised or potentially compromised by the breach;
- (5) The number of District residents affected or estimated to be 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) Any remedial action taken or proposed to be taken by the person or entity that experienced the breach; and
- (8) A generic copy 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.

Bill 23-215, "Security Breach Protection Amendment Act of 2020"

Committee of the Whole

Draft Comparative Print

(e) Notwithstanding subsection (a) of this section, a person or ~~entity business~~ that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or ~~entity business~~ provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter. Notice under this section may be given by electronic mail if the person or entity's primary method of communication with the resident is by electronic means. The person or entity, in all cases, shall provide written notice of the breach of the security of the system to the Office of the Attorney General as required under subsection (b-1) of this section.

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

(g) A person or entity who 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.) ("Act"), and provides notice in accordance with the Act, 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. But the person or entity, in all cases, shall provide written notice of the breach of the security of the system to the Office of the Attorney General as required under subsection (b-1) of this section.

Sec. 28-2852a. Security requirements.

(a) To protect personal information from unauthorized access, use, notification, disclosure or a reasonably anticipated hazard or threat, a person or entity that owns, licenses, maintains, handles, or otherwise possesses personal information of an individual residing in the District shall implement and maintain reasonable security safeguards, including procedures and practices, that are appropriate to the nature of the personal information and the nature and size of the entity or operation.

(b) A person or entity that uses a nonaffiliated third party as a service provider to perform services for a person or entity and discloses person information about an individual residing in the District under a written agreement with the third party shall require by the agreement that the third party implement and maintain reasonable security procedures and practices that:

(1) Are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and

(2) Are reasonably designed to protect the personal information from unauthorized access, use, modification, and disclosure.

(c) When a person or entity is destroying records, including computerized or electronic records and devices containing computerized or electronic records, that contain personal information of a consumer, employee, or former employee of the person or entity, the person or entity shall take

**Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print**

reasonable steps to protect against unauthorized access to or use of the personal information, taking into account:

- (1) The sensitivity of the records;
- (2) The nature and size of the business and its operations;
- (3) The costs and benefits of different destruction and sanitation methods; and
- (4) Available technology.

(d) A person or entity who is subject to and in compliance with requirements for security procedures and practices contained in Title V of the Gramm-Leach-Bliley Act, approved November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 *et seq.*), and any rules, regulations, guidance and guidelines thereto, shall be deemed to be in compliance with this section.

Sec. 28-2852b. Remedies.

When a person or entity experiences a breach of the security of the system that requires notification under subsection § 28-3852(a) or (b), and such breach includes or is reasonably believed to include a social security number or taxpayer identification number, the person or entity shall offer identity theft protection services to each District resident whose social security number or tax identification number was released at no costs to such District resident for a period of not less than 18 months. The person or entity that experienced the breach of the security of its system shall provide all information necessary for District residents to enroll in the services required under this subsection.

Sec. 28-2852c. Rulemaking.

The Attorney General for the District of Columbia, pursuant to § 2-501 *et seq.* may issue rules to implement the notification provisions pursuant to section 28-3852.

§ 28–3853. Enforcement.

~~(a) Any District of Columbia resident injured by a violation of this subchapter 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.~~

~~(b) A violation of this act, or any rule issued pursuant to the authority of this act, is an unfair or deceptive trade practice pursuant to section 28-3904(kk). The Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and for an award of restitution for property lost or damages suffered by District of Columbia residents as a consequence of the violation of this subchapter. In an action under this subsection, the Attorney~~

**Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print**

~~General may recover a civil penalty not to exceed \$100 for each violation, the costs of the action, and reasonable attorney’s fees. Each failure to provide a District of Columbia resident with notification in accordance with this section shall constitute a separate violation.~~

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

**District of Columbia Consumer Protection Procedures Act
(D.C. OFFICIAL CODE § 28-3901 *ET SEQ.*)**

§ 28–3904. Unfair or deceptive trade practices.

It shall be a violation of this chapter for any person to engage in an unfair or deceptive trade practice, whether or not any consumer is in fact misled, deceived, or damaged thereby, including to:

- (a) represent that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- (b) represent that the person has a sponsorship, approval, status, affiliation, certification, or connection that the person does not have;
- (c) represent that goods are original or new if in fact they are deteriorated, altered, reconditioned, reclaimed, or second hand, or have been used;
- (d) represent that goods or services are of particular standard, quality, grade, style, or model, if in fact they are of another;
- (e) misrepresent as to a material fact which has a tendency to mislead;
- (e-1) [r]epresent that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law;
- (f) fail to state a material fact if such failure tends to mislead;
- (f-1) [u]se innuendo or ambiguity as to a material fact, which has a tendency to mislead;
- (g) disparage the goods, services, or business of another by false or misleading representations of material facts;
- (h) advertise or offer goods or services without the intent to sell them or without the intent to sell them as advertised or offered;

Bill 23-215, "Security Breach Protection Amendment Act of 2020"

Committee of the Whole

Draft Comparative Print

(i) advertise or offer goods or services without supplying reasonably expected public demand, unless the advertisement or offer discloses a limitation of quantity or other qualifying condition which has no tendency to mislead;

(j) make false or misleading representations of fact concerning the reasons for, existence of, or amounts of price reductions, or the price in comparison to price of competitors or one's own price at a past or future time;

(k) falsely state that services, replacements, or repairs are needed;

(l) falsely state the reasons for offering or supplying goods or services at sale or discount prices;

(m) harass or threaten a consumer with any act other than legal process, either by telephone, cards, letters, or any form of electronic or social media;

(n) cease work on, or return after ceasing work on, an electrical or mechanical apparatus, appliance, chattel or other goods, or merchandise, in other than the condition contracted for, or to impose a separate charge to reassemble or restore such an object to such a condition without notification of such charge prior to beginning work on or receiving such object;

(o) replace parts or components in an electrical or mechanical apparatus, appliance, chattel or other goods, or merchandise when such parts or components are not defective, unless requested by the consumer;

(p) falsely state or represent that repairs, alterations, modifications, or servicing have been made and receiving remuneration therefor when they have not been made;

(q) fail to supply to a consumer a copy of a sales or service contract, lease, promissory note, trust agreement, or other evidence of indebtedness which the consumer may execute;

(r) make or enforce unconscionable terms or provisions of sales or leases; in applying this subsection, consideration shall be given to the following, and other factors:

(1) knowledge by the person at the time credit sales are consummated that there was no reasonable probability of payment in full of the obligation by the consumer;

(2) knowledge by the person at the time of the sale or lease of the inability of the consumer to receive substantial benefits from the property or services sold or leased;

(3) gross disparity between the price of the property or services sold or leased and the value of the property or services measured by the price at which similar property or services are readily obtainable in transactions by like buyers or lessees;

(4) that the person contracted for or received separate charges for insurance with respect to credit sales with the effect of making the sales, considered as a whole, unconscionable; and

Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print

(5) that the person has knowingly taken advantage of the inability of the consumer reasonably to protect his interests by reasons of age, physical or mental infirmities, ignorance, illiteracy, or inability to understand the language of the agreement, or similar factors;

(s) pass off goods or services as those of another;

(t) use deceptive representations or designations of geographic origin in connection with goods or services;

(u) represent that the subject of a transaction has been supplied in accordance with a previous representation when it has not;

(v) misrepresent the authority of a salesman, representative or agent to negotiate the final terms of a transaction;

(w) offer for sale or distribute any consumer product which is not in conformity with an applicable consumer product safety standard or has been ruled a banned hazardous product under the federal Consumer Product Safety Act (15 U.S.C. § 2051-83), without holding a certificate issued in accordance with section 14(a) of that Act to the effect that such consumer product conforms to all applicable consumer product safety rules (unless the certificate holder knows that such consumer product does not conform), or without relying in good faith on the representation of the manufacturer or a distributor of such product that the product is not subject to a consumer product safety rule issued under that Act;

(x) sell consumer goods in a condition or manner not consistent with that warranted by operation of sections 28:2-312 through 318 of the District of Columbia Official Code, or by operation or requirement of federal law;

(y) violate any provision of the District of Columbia Consumer LayAway Plan Act (section 28-3818);

(z) violate any provision of the Rental Housing Locator Consumer Protection Act of 1979 (section 28-3819) or, if a rental housing locator, to refuse or fail to honor any obligation under a rental housing locator contract;

(z-1) violate any provision of [Chapter 46 of this title](#);

(aa) violate any provision of sections 32-404, 32-405, 32-406, and 32-407;

(bb) refuse to provide the repairs, refunds, or replacement motor vehicles or fails to provide the disclosures of defects or damages required by the Automobile Consumer Protection Act of 1984;

(cc) violate any provision of the Real Property Credit Line Deed of Trust Act of 1987;

(dd) violate any provision of title 16 of the District of Columbia Municipal Regulations;

Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print

(ee) violate any provision of the Public Insurance Adjuster Act of 2002 [[Chapter 16A of Title 31](#)];

(ff) violate any provision of [Chapter 33 of this title](#);

(gg) violate any provision of the Home Equity Protection Act of 2007 [[Chapter 24A of Title 42](#)];

(hh) fail to make a disclosure as required by [§ 26-1113\(a-1\)](#);

(ii) violate any provision of [Chapter 53 of this title](#); ~~or~~

(jj) violate any agreement entered into pursuant to [section 28-3909\(c\)\(6\)](#); or

~~(kk) violate any provision of subchapter 2 of Chapter 38 of this title. -~~

§ 28–3909. Restraining prohibited acts.

(a) Notwithstanding any provision of law to the contrary, if the Attorney General for the District of Columbia has reason to believe that any person is using or intends to use any method, act, or practice in violation of section [28-3803](#), [28-3805](#), [28-3807](#), [28-3810](#), [28-3811](#), [28-3812](#), [28-3814](#), [28-3817](#), [28-3818](#), [28-3819](#), [28-3851](#), [28-3852](#), [28-3852a](#), [28-3852b](#) or [28-3904](#), and if it is in the public interest, the Attorney General, in the name of the District of Columbia, may bring an action in the Superior Court of the District of Columbia to obtain a temporary or permanent injunction prohibiting the use of the method, act, or practice and requiring the violator to take affirmative action, including the restitution of money or property. In any action under this section, the Attorney General shall not be required to prove damages and the injunction shall be issued without bond.

(b) In addition, in an action under this section, the Attorney General for the District of Columbia may recover:

(1) From a merchant who engaged in a first violation of section [28-3803](#), [28-3805](#), [28-3807](#), [28-3810](#), [28-3811](#), [28-3812](#), [28-3814](#), [28-3817](#), [28-3818](#), [28-3819](#), [28-3851](#), [28-3852](#), [28-3852a](#), [28-3852b](#) or [28-3904](#), a civil penalty of not more than \$5,000 for each violation;

(2) From a merchant who engaged in a first violation of section [28-3803](#), [28-3805](#), [28-3807](#), [28-3810](#), [28-3811](#), [28-3812](#), [28-3814](#), [28-3817](#), [28-3818](#), [28-3819](#), [28-3851](#), [28-3852](#), [28-3852a](#), [28-3852b](#) or [28-3904](#) and who subsequently repeats the same violation, a civil penalty of not more than \$10,000 for each subsequent violation;

(3) Economic damages; and

(4) The costs of the action and reasonable attorneys' fees.

(c) The Attorney General for the District of Columbia may also:

Bill 23-215, “Security Breach Protection Amendment Act of 2020”
Committee of the Whole
Draft Comparative Print

- (1) represent the interests of consumers before administrative and regulatory agencies and legislative bodies;
 - (2) assist, advise, and cooperate with private, local, and federal agencies and officials to protect and promote the interests of consumers;
 - (3) assist, develop, and conduct programs of consumer education and information through public hearings, meetings, publications, or other materials prepared for distribution to consumers;
 - (4) undertake activities to encourage local business and industry to maintain high standards of honesty, fair business practices, and public responsibility in the production, promotion, and sale of consumer goods and services and in the extension of consumer credit;
 - (5) perform other functions and duties which are consistent with the purposes or provisions of this chapter, and with the Attorney General's role as *parens patriae*, which may be necessary or appropriate to protect and promote the welfare of consumers;
 - (6) negotiate and enter into agreements for compliance by merchants with the provisions of this chapter; or
 - (7) publicize its own actions taken in the interests of consumers.
- (d) The Attorney General for the District of Columbia may apply the provisions and exercise the duties of this section to landlord-tenant relations.

1 **DRAFT COMMITTEE PRINT**
2 Committee of the Whole
3 January 21, 2020
4
5
6
7

8 A BILL

9 23-215
10 _____
11

12 IN THE COUNCIL OF THE DISTRICT OF COLUMBIA
13 _____
14

15 To amend Title 28 of the District of Columbia Official Code concerning businesses’ data breaches
16 to expand definitions, to specify the required contents of a notification of a security breach
17 to a person whose personal information is included in a breach, to clarify timeframes for
18 reporting breaches, to require that written notice of the breach, including specific
19 information, be given to the Office of the Attorney General, to specify the security
20 requirements for the protection of personal information, to require the provision of 18
21 months of identity theft prevention services when the breach results in the release of social
22 security or tax identification numbers, to make violation of the requirements for protection
23 of personal information an unfair or deceptive trade practice, and to make a conforming
24 amendment to the Consumer Protection Procedures Act.
25

26 BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this
27 act may be cited as the “Security Breach Protection Amendment Act of 2020”.

28 Sec. 2. Title 28, Chapter 38 of the District of Columbia Official Code is amended as
29 follows:

30 (a) Section 28-3801 is amended by striking the word “chapter” and inserting the word
31 “subchapter” in its place.

32 (b) The table of contents for subchapter 2 is amended by adding three new section
33 designations to read as follows:

34 “§ 28-3852a. Security Requirements.

35 “§ 28-3852b. Remedies.

36 “§ 28-3852c. Rulemaking.”.

37 (c) Section 28-3851 is amended as follows:

38 (1) Paragraph (1) is amended to read as follows:

39 “(1)(A) “Breach of the security of the system” means unauthorized acquisition of
40 computerized or other electronic data or any equipment or device storing such data that
41 compromises the security, confidentiality, or integrity of personal information maintained by the
42 person or entity who conducts business in the District of Columbia.

43 “(B) The term “breach of the security of the system” does not include:

44 “(i) A good faith acquisition of personal information by an employee
45 or agency of the person or entity for the purposes of the person or entity if the personal information
46 is not used improperly or subject to further unauthorized disclosure;

47 “(ii) Acquisition of data that has been rendered secure so as to be
48 unusable by an unauthorized third party unless any information obtained has the potential to
49 compromise the effectiveness of the security protection preventing unauthorized access; or

50 “(iii) Acquisition of personal information of an individual that the
51 person or entity reasonably determines, after consultation with District and federal law
52 enforcement agencies, will likely not result in harm to the individual.

53 (2) New paragraphs (1A) and (1B) are added to read as follows:

54 “(1A) “Genetic information” has the meaning ascribed to it under the federal Health
55 Insurance Portability and Accountability Act of 1996 (“HIPAA”), approved August 21, 1996 (Pub.
56 Law 104-191; 110 Stat. 1936), as specified in 45 C.F.R. § 106.103.

57 “(1B) “Medical Information” means any information about a consumer’s dental,
58 medical or mental health treatment or diagnosis by a health care professional.”.

59 (3) Paragraph (2) is amended by striking the word “business” wherever it appears
60 and inserting the word “entity” in its place.

61 (4) A new paragraph (2A) is added to read as follows:

62 “(2A) “Person or entity” means an individual, firm, corporation, partnership,
63 company, cooperative, association, trust, or any other organization, legal entity, or group of
64 individuals. The term “person or entity” shall not include the District of Columbia government or
65 any of its agencies or instrumentalities.”.

66 (5) Paragraph (3) is amended to read as follows:

67 “(3)(A) "Personal information" means:

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

71 “(I) Social security number, Individual Taxpayer
72 Identification Number, passport number, driver’s license number, military identification number,
73 or other identifier issued by the District of Columbia or any local, state or federal government
74 agency;

75 “(II) Account number, credit card number or debit card
76 number, or any other number or code or combination of numbers or codes, such as an identification

77 number, account number, security code, access code, or password, that allows access to or use of
78 an individual's financial or credit account;

79 “(III) Medical information;

80 “(IV) Genetic information and deoxyribonucleic acid
81 profile;

82 “(V) Health insurance information, including a policy
83 number, subscriber information number, or any unique identifier used by a health insurer to
84 identify the person that permits access to an individual’s health and billing information;

85 “(VI) Biometric data of an individual generated by automatic
86 measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic
87 print, retina or iris image, or other unique biological characteristic, that can be used to uniquely
88 authenticate the individual's identity when the individual accesses a system or account; or

89 “(VII) Any combination of data elements included in sub-
90 sub-sub paragraphs (I) through (VI) of this sub-subparagraph that would enable a person to commit
91 identity theft without reference to a person’s first name or first initial and last name or other
92 independent personal identifier.

93 “(ii) A user name or e-mail address in combination with a password,
94 security question and answer or other means of authentication, or any combination of data elements
95 included in sub-sub-sub paragraphs (I) through (VI) that permits access to an individual's e-mail
96 account.”.

97 (d) Section 28-3852 is amended as follows:

98 (1) New subsections (a-1) and (a-2) are added to read as follows:

99 “(a-1) The notification required under subsection (a) of this section shall include:

100 “(1) To the extent possible, a description of the categories of information
101 that were, or are reasonably believed to have been, acquired by an unauthorized person, including
102 the elements of personal information that were, or are reasonably believed to have been, acquired;

103 “(2) Contact information for the person or entity making the notification,
104 including the business address, telephone number, and toll-free telephone number if one is
105 maintained;

106 “(3) The toll-free telephone numbers and addresses for the major consumer
107 reporting agencies, including a statement notifying the resident of the right to obtain a security
108 freeze free of charge pursuant to 15 U.S.C. § 1681c-1 and information how a resident may request
109 a security freeze; and

110 “(4) The toll-free telephone numbers, addresses, and website addresses for
111 the following entities, including a statement that an individual can obtain information from these
112 sources about steps to take to avoid identity theft:

113 “(A) The Federal Trade Commission; and

114 “(B) The Office of the Attorney General for the District of
115 Columbia.”.

116 “(a-2) Notwithstanding subsection (a-1), in the case of a breach of the security of
117 the system that only involves personal information defined in section 28-3851(3)(A)(ii), the person
118 or entity may comply with this section by providing the notification in electronic format or other
119 form that directs the person to change the person’s password and security question or answer, as
120 applicable, or to take other steps appropriate to protect the e-mail account with the person or entity
121 and all other online accounts for which the person whose personal information has been breached
122 uses the same username or email address and password or security question or answer.

123 (2) New subsections (b-1) and (b-2) are added to read as follows:

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

130 “(1) The name and contact information of the person or entity reporting the
131 breach;

132 “(2) The name and contact information of the person or entity that
133 experienced the breach;

134 “(3) The nature of the breach of the security of the system, including the
135 name of the person or entity that experienced the breach;

136 “(4) The types of personal information compromised by the breach;

137 “(5) The number of District residents affected by the breach;

138 “(6) The cause of the breach, including the relationship between the person
139 or entity that experienced the breach and the person responsible for the breach, if known;

140 “(7) Any remedial action taken by the person or entity;

141 “(8) The date and time frame of the breach, if known;

142 “(9) Address and location of corporate headquarters, if outside of the
143 District;

144 “(10) Any knowledge of foreign country involvement; and

145 “(11) A sample of the notice to be provided to District residents.

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

149 (3) Subsection (e) is amended as follows:

150 (A) Strike the phrase “a person or business that” and insert the
151 phrase “a person or entity that” in its place.

152 (B) Strike the phrase “the person or business provides” and insert
153 the phrase “the person or entity provides” in its place.

154 (C) Insert the following sentence at the end: “The person or entity
155 shall, in all cases, provide written notice of the breach of the security of the system to the Office
156 of the Attorney General as required under subsection (b-1) of this section.”

157 (4) Subsection (g) is amended by striking the phrase “with this section” and
158 inserting the phrase “with this section with respect to the notification of residents whose personal
159 information is included in the breach. The person or entity shall, in all cases, provide written notice
160 of the breach of the security of the system to the Office of the Attorney General as required under
161 subsection (b-1) of this section.” in its place.

162 (e) New sections 28-3852a and 28-3852b, and 28-3852c are added to read as follows:

163 “§ 28-3852a. Security requirements.

164 “(a) To protect personal information from unauthorized access, use, modification,
165 disclosure or a reasonably anticipated hazard or threat, a person or entity that owns, licenses,
166 maintains, handles or otherwise possesses personal information of an individual residing in the
167 District shall implement and maintain reasonable security safeguards, including procedures and

168 practices that are appropriate to the nature of the personal information and the nature an size of the
169 entity or operation.

170 “(b) A person or entity that uses a nonaffiliated third party as a service provider to perform
171 services for a person or entity and discloses personal information about an individual residing in
172 the District under a written agreement with the third party shall require by the agreement that the
173 third party implement and maintain reasonable security procedures and practices that:

174 “(1) Are appropriate to the nature of the personal information disclosed to the
175 nonaffiliated third party; and

176 “(2) Are reasonably designed to protect the personal information from unauthorized
177 access, use, modification, and disclosure.

178 “(c) When a person or entity is destroying records, including computerized or electronic
179 records and devices containing computerized or electronic records, that contain personal
180 information of a consumer, employee, or former employee of the person or entity, the person or
181 entity shall take reasonable steps to protect against unauthorized access to or use of the personal
182 information, taking into account:

183 “(1) The sensitivity of the records;

184 “(2) The nature and size of the business and its operations;

185 “(3) The costs and benefits of different destruction and sanitation methods; and

186 “(4) Available technology.

187 “(d) A person or entity who is subject to and in compliance with requirements for security
188 procedures and practices contained in Title V of the Gramm-Leach-Bliley Act, approved
189 November 12, 1999 (113 Stat. 1436; 15 U.S.C. § 6801 *et seq.*), and any rules, regulations,
190 guidance and guidelines thereto, shall be deemed to be in compliance with this section.”.

191 “§ 28-3852b. Remedies.

192 “When a person or entity experiences a breach of the security of the system that requires
193 notification under subsection 28-3852(a) or (b), and such breach includes or is reasonably believed
194 to include a social security number or taxpayer identification number, the person or entity shall
195 offer to each District resident whose social security number or tax identification number was
196 released identity theft protection services at no cost to such District resident for a period of not less
197 than 18 months. The person or entity that experienced the breach of the security of its system shall
198 provide all information necessary for District residents to enroll in the services required under this
199 subsection.

200 “§ 28-3852c. Rulemaking.

201 “The Attorney General for the District of Columbia, pursuant to section 2-501 *et seq.* may
202 issue rules to implement the notification provisions pursuant to section 28-3852.”.

203 (f) Section 28-3853 is amended as follows:

204 (1) Subsection (a) is repealed.

205 (2) Subsection (b) is amended to read as follows:

206 “(b) A violation of this act, or any rule issued pursuant to the authority of this act, is an
207 unfair or deceptive trade practice pursuant to section 28-3904(kk).”.

208 (g) Section 28-3904 is amended as follows:

209 (1) Subsection (ii) is amended by striking the word “or”.

210 (2) Subsection (jj) is amended by striking the period and inserting the phrase “; or”
211 in its place.

212 (3) A new subsection (kk) is added to read as follows:

213 “(kk) violate any provision of subchapter 2 of Chapter 38 of this title.”.

214 (h) Section 28-3909 is amended by striking the phrase “28-3819 or 28-3904” wherever it
215 appears and inserting the phrase “28-3819, 28-3851, 28-3852, 28-3852a, 28-3852b or 28-3904” in
216 its place.

217 Sec. 3. Fiscal impact statement.

218 The Council adopts the fiscal impact statement of the Chief Financial Officer as the fiscal
219 impact statement required by section 602(c)(3) of the District of Columbia Home Rule Act,
220 approved December 24, 1973 (87 Stat. 813; D.C. Official Code §1-206.02(c)(3)).

221 Sec. 4. Effective date.

222 This act shall take effect following approval by the Mayor (or in the event of veto by the
223 Mayor, action by the Council to override the veto), a 30-day period of congressional review as
224 provided in 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973
225 (87 Stat. 813; D.C. Official Code §1-206.02(c)(1)), and publication in the District of Columbia
226 Register.

227

228