Attachment #43

Bill # 2020 - - H 7723, An Act Relating to Commercial Law – General Regulatory Provisions – Establishing the Consumer Personal Data Protection Act of 2020

2020 -- H 7723

LC005062

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2020

AN ACT

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- ESTABLISHING THE "CONSUMER PERSONAL DATA PROTECTION ACT OF 2020"

Introduced By: Representatives Edwards, Shanley, Barros, Cassar, and Carson

Date Introduced: February 26, 2020

Referred To: House Judiciary

It is enacted by the General Assembly as follows:

SECTION 1. Title 6 of the General Laws entitled "COMMERCIAL LAW - GENERAL REGULATORY PROVISIONS" is hereby amended by adding thereto the following chapter:

CHAPTER 48.1

CONSUMER PERSONAL DATA PROTECTION ACT OF 2020

6-48.1-1. Short title.

This chapter shall be known and may be cited as the "Consumer Personal Data Protection Act of 2020."

6-48.1-2. Legislative findings and intent.

(a) The general assembly hereby finds that:

(1) It serves the best interest of the public to provide consumers with more information about data brokers, and their data collection practices:

(i) While many different types of businesses collect data about consumers, a "data broker" is in the business of aggregating and selling data about consumers with whom the business does not have a direct relationship;

(ii) A data broker collects many hundreds or thousands of data points about consumers from multiple sources, including: Internet browsing history; online purchases; public records; location data; loyalty programs; and subscription information. The data broker then scrubs the data to ensure accuracy; analyzes the data to assess content; and packages the data for sale to a third

party;

(iii) Data brokers provide information that is critical to services offered in the modern economy, including: targeted marketing and sales; credit reporting; background checks; government information; risk mitigation and fraud detection; people search; decisions by banks, insurers, or others whether to provide services; ancestry research, and voter targeting and strategy by political campaigns;

(iv) While data brokers offer many benefits, there are also risks associated with the widespread aggregation and sale of data about consumers, including risks related to consumers' ability to know and control information held and sold about them and risks arising from the unauthorized or harmful acquisition and use of consumer information;

(v) There are important differences between "data brokers" and businesses with whom consumers have a direct relationship;

(A) Consumers who have a direct relationship with traditional and e-commerce businesses may have some level of knowledge about and control over the collection of data by those businesses, including: the choice to use the business's products or services; the ability to review and consider data collection policies; the ability to opt-out of certain data collection practices; the ability to identify and contact customer representatives; the ability to pursue contractual remedies through litigation; and the knowledge necessary to file a complaint with law enforcement;

(B) By contrast, consumers may not be aware that data brokers exist, who the companies are, or what information they collect, and may not be aware of available recourse;

(vi) The state of Rhode Island has the legal authority and duty to exercise its traditional "police powers" to ensure the public health, safety, and welfare, which includes both the right to regulate businesses that operate in the state and engage in activities that affect Rhode Island consumers as well as the right to require disclosure of information to protect consumers from harm;

(vii) To provide consumers with necessary information about data brokers, Rhode Island adopts a narrowly tailored definition of "data broker" and requires data brokers to register annually with the secretary of state and provide information about their data collection activities, opt-out policies, purchaser credentialing practices, and security breaches;

(2) The public interest requires that data brokers have adequate security standards:

(i) News headlines in the past several years demonstrate that large and sophisticated businesses, governments, and other public and private institutions are constantly subject to cyberattacks, which have compromised sensitive personal information of literally billions of consumers worldwide;

(ii) While neither government nor industry can prevent every security breach, the state of

Rhode Island has the authority and the duty to enact legislation to protect its consumers where possible;

(iii) One approach to protecting consumer data has been to require government agencies and certain regulated businesses to adopt an "information security program" that has "appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records" and "to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm." Federal Privacy Act, 5 U.S.C. § 552a;

(iv) The requirement to adopt such an information security program currently applies to "financial institutions" subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. to persons who maintain or transmit health information regulated by the Health Insurance Portability and Accountability Act, and to various types of businesses under laws in at least thirteen (13) other states;

(v) Rhode Island can better protect its consumers from data broker security breaches and related harm by requiring data brokers to adopt an information security program with appropriate administrative, technical, and physical safeguards to protect sensitive personal information;

(3) A need exists to prohibit the acquisition of personal information through fraudulent means or with the intent to commit wrongful acts;

(i) One of the dangers of the broad availability of sensitive personal information is that it can be used with malicious intent to commit wrongful acts, such as stalking, harassment, fraud, discrimination, and identity theft;

(ii) While various criminal and civil statutes prohibit these wrongful acts, there is currently no prohibition on acquiring data for the purpose of committing such acts;

(iii) Rhode Island hereby creates new causes of action to prohibit the acquisition of personal information through fraudulent means, or for the purpose of committing a wrongful act, to enable authorities and consumers to take action;

(4) The removal of financial barriers will protect consumer credit information;

(i) In one of several major security breaches that have occurred in recent years, the names, social security numbers, birth dates, addresses, driver's license numbers, and credit card numbers of over one hundred forty-five million (145,000,000) Americans were exposed, including citizens of Rhode Island;

(ii) In response to concerns about data security, identity theft, and consumer protection, one important step a consumer can take is to place a security freeze on their credit file with each of the national credit reporting agencies;

(iii) Pursuant to § 6-48-5, when a consumer places a security freeze, a credit reporting

agency issues a unique personal identification number (PIN) or password to the consumer. The consumer must provide the PIN or password, and their express consent, to allow a potential creditor to access their credit information;

(iv) Rhode Island prohibits these fees to eliminate any financial barrier to placing or removing a security freeze.

(b) The intent of the general assembly is the protection of consumer personal data by:

(1) Providing consumers with more information about data brokers, their data collection practices, and the right to opt-out. It is the intent of the general assembly to provide citizens of Rhode Island with access to more information about the data brokers that collect consumer data and their collection practices by:

(i) Adopting a narrowly tailored definition of "data broker" that:

(A) Includes only those businesses that aggregate and sell the personal information of consumers with whom they do not have a direct relationship; and

(B) Excludes businesses that collect information from their own customers, employees, users, or donors, including: banks and other financial institutions; utilities; insurers; retailers and grocers; restaurants and hospitality businesses; social media websites and mobile "apps"; search websites; and businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as a website, "app," and e-commerce platforms; and

(ii) Requiring a data broker to register annually with the secretary of state and make certain disclosures in order to provide consumers, policy makers, and regulators with relevant information;

(2) Ensuring that data brokers have adequate security standards. It is the intent of the general assembly to protect against potential cyber threats by requiring data brokers to adopt an information security program with appropriate technical, physical, and administrative safeguards;

(3) Prohibiting the acquisition of personal information with the intent to commit wrongful acts. It is the intent of the general assembly to protect citizens of Rhode Island from potential harm by creating new causes of action that prohibit the acquisition or use of personal information for the purpose of stalking, harassment, fraud, identity theft, or discrimination; and

(4) Removing financial barriers to protect consumer credit information. It is the intent of the general assembly to remove any financial barrier for citizens of Rhode Island who intend to place a security freeze on their credit report by prohibiting credit reporting agencies from charging a fee to place or remove a freeze.

6-48.1-3. Definitions.

As used in this chapter:

(1) "Brokered personal information" means one or more of the following computerized

data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) Name;

(ii) Address;

(iii) Date of birth;

(iv) Place of birth;

(v) Mother's maiden name;

(vi) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii) Name or address of a member of the consumer's immediate family or household;

(viii) Social security number or other government-issued identification number; or

(ix) Other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty; however, it does not include publicly available information to the extent that it is related to a consumer's business or profession;

(2) "Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the state of Rhode Island, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the state of Rhode Island, a state agency, any political subdivision of the state of Rhode Island, or a vendor acting solely on behalf of, and at the direction of, the state of Rhode Island;

(3) "Consumer" means an individual residing in this state;

(4)(i) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship;

(ii) Examples of a direct relationship with a business include if the consumer is a past or present:

(A) Customer, client, subscriber, user, or registered user of the business's goods or services;

(B) Employee, contractor, or agent of the business;

(C) Investor in the business; or

(D) Donor to the business.

(iii) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

(A) Developing or maintaining third-party e-commerce or application platforms;

(B) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(C) Providing publicly available information related to a consumer's business or profession; or

(D) Providing publicly available information via real-time or near-real-time alert services for health or safety purposes;

(iv) The phrase "sells or licenses" does not include:

(A) A one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(B) A sale or license of data that is merely incidental to the business;

(5)(i) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person;

(ii) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure;

(iii) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

(A) Indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;

(B) Indications that the brokered personal information has been downloaded or copied;

(C) Indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(D) That the brokered personal information has been made public;

(6) "Data collector" means a person who, for any purpose, whether by automated collection

or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the state of Rhode Island, state agencies, political subdivisions of the state, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators;

(7) "Encryption" or "Encrypted" means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data. These terms shall also mean any security solution, other than a one hundred twenty-eight (128) bit or higher algorithmic process that provides the same degree or higher degree of security;

(8) "License" means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license;

(9) "Personally identifiable information" or "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format:

(i) Social security number;

(ii) Driver's license number, passport number, Rhode Island identification card number, or tribal identification number;

(iii) Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account;

(iv) Medical or health insurance information; or

(v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(10) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics;

(11) "Redaction" means the rendering of data in a form that renders the data unreadable or is truncated resulting in no more than the last four (4) digits of the identification number are accessible as part of the data;

(12)(i) "Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of, electronic data that compromises the security,

confidentiality, or integrity of a consumer's personally identifiable information maintained by a data collector;

(ii) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure;

(iii) In determining whether personally identifiable information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(A) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;

(B) Indications that the information has been downloaded or copied;

(C) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(D) That the information has been made public.

6-48.1-4. Restricted acquisition of brokered personal information.

(a) Prohibited acquisition and use:

(1) A person shall not acquire brokered personal information through fraudulent means;

(2) A person shall not acquire or use brokered personal information for the purpose of:

(i) Stalking or harassing another person;

(ii) Committing a fraud, including identity theft, financial fraud, or email fraud; or

(iii) Engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(b) Promulgation of rules and prohibited practices:

(1) A person who violates a provision of this section commits a deceptive trade practice in violation of chapter 13.1 of title 6;

(2) The director of the department of business regulations shall promulgate rules to implement the provisions of this chapter.

6-48.1-5. Annual registration.

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in this chapter, the data broker shall:

(1) Register with the secretary of state;

(2) Pay a registration fee of one hundred dollars ($100); and

(3) Provide the following information:

(i) The name and primary physical, email, and Internet address(es) of the data broker;

(ii) If the data broker permits a consumer to opt-out of the data broker's collection of brokered personal information, opt-out of its databases, or opt-out of certain sales of data:

(A) The method for requesting an opt-out;

(B) If the opt-out applies to only certain activities or sales, identification of which ones; and

(C) Whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(iii) A statement specifying the data collection, databases, or sales activities from which a consumer may not opt-out;

(iv) A statement whether the data broker implements a purchaser credentialing process;

(v) The number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(vi) Where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(vii) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable for:

(1) A civil penalty of fifty dollars ($50.00) for each day, not to exceed a total of ten thousand dollars ($10,000) for each year, it fails to register pursuant to this section;

(2) An amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) Other penalties imposed by law.

(c) The attorney general may maintain an action in superior court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

6-48.1-6. Duty to protect information.

(a) Duty to protect personally identifiable information:

(1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(i) The size, scope, and type of business of the data broker obligated to safeguard the

personally identifiable information under such comprehensive information security program;

(ii) The amount of resources available to the data broker;

(iii) The amount of stored data; and

(iv) The need for security and confidentiality of personally identifiable information;

(2) A data broker subject to this chapter shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other state rules or federal regulations applicable to the data broker.

(b) Information security program - minimum features. A comprehensive information security program shall at minimum have the following features:

(1) Designation of one or more employees to maintain the program;

(2) Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(i) Ongoing employee training, including training for temporary and contract employees;

(ii) Employee compliance with policies and procedures; and

(iii) Means for detecting and preventing security system failures;

(3) Security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises;

(4) Disciplinary measures for violations of the comprehensive information security program rules;

(5) Measures that prevent terminated employees from accessing records containing personally identifiable information;

(6) Supervision of service providers, by:

(i) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and

(ii) Requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information;

(7) Reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers;

(8)(i) Regular monitoring to ensure that the comprehensive information security program

is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and

(ii) Upgrading information safeguards as necessary to limit risks;

(9) Regular review of the scope of the security measures:

(i) At least annually; or

(ii) Whenever there is a material change in business practices that may reasonably affect the security or integrity of records containing personally identifiable information; and

(10)(i) Documentation of responsive actions taken in connection with any incident involving a breach of security; and

(ii) Mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

(c) Information security program; computer system security requirements. A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, have the following elements:

(1) Secure user authentication protocols, as follows:

(i) An authentication protocol that has the following features:

(A) Control of user identifications and other identifiers;

(B) A reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(C) Control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the protected data;

(D) Restricting access to only active users and active user accounts; and

(E) Blocking access to user identification after multiple unsuccessful attempts to gain access; or

(ii) An authentication protocol that provides a higher level of security than the features specified in this subsection.

(2) Secure access control measures that:

(i) Restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(ii) Assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) Encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally

identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) Reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

(5) Encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) For files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

(7) Reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) Education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security.

(d) Enforcement.

(1) A person who violates a provision of this chapter commits a deceptive trade practice in violation of chapter 13.1 of title 6.

(2) The attorney general has the authority to conduct civil investigations, and bring civil actions as provided in § 6-13.1-5.

(3) Nothing in this chapter shall be construed to authorize any private right of action to enforce any provision of this chapter, any regulation hereunder, or any other provisions of commercial law in title 6.

6-48.1-7. Disclosure to consumers.

(a) A credit reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer all information available to users at the time of the request pertaining to the consumer, including:

(1) Any credit score or predictor relating to the consumer, in a form and manner that complies with such comments or guidelines as may be issued by the Federal Trade Commission;

(2) The names of users requesting information pertaining to the consumer during the prior twelve (12) month period and the date of each request; and

(3) A clear and concise explanation of the information.

(b) As frequently as new telephone directories are published, the credit reporting agency shall cause to be listed its name and number in each telephone directory published to serve communities of this state. In accordance with rules adopted by the attorney general, the credit reporting agency shall make provision for consumers to request by telephone the information required to be disclosed pursuant to subsection (a) of this section at no cost to the consumer.

(c) Any time a credit reporting agency is required to make a written disclosure to consumers pursuant to 15 U.S.C. § 1681g, it shall disclose, in at least twelve (12) point type, and in bold type as indicated, the following notice:

"NOTICE TO RHODE ISLAND CONSUMERS

You are allowed to receive one free copy of your credit report every twelve (12) months from each credit reporting agency.

Under Rhode Island law, no one may access your credit report without your permission except under the following limited circumstances:

(1) In response to a court order;

(2) For direct mail offers of credit;

(3) If you have given ongoing permission and you have an existing relationship with the person requesting a copy of your credit report;

(4) Where the request for a credit report is related to an education loan made, guaranteed, or serviced by the Rhode Island student loan authority;

(5) Where the request for a credit report is by the office of child support services when investigating a child support case;

(6) Where the request for a credit report is related to a credit transaction entered into prior to January 1, 1993; and/or

(7) Where the request for a credit report is by the Rhode Island division of taxation and is used for the purpose of collecting or investigating delinquent taxes.

If you believe a law regulating consumer credit reporting has been violated, you may file a complaint with the state of Rhode Island attorney general.

Consumers Have the Right to Obtain a Security Freeze.

You have a right to place a "security freeze" on your credit report pursuant to Rhode Island general laws § 6-48-5 at no charge. The security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail.

The security freeze is designed to help prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security

freeze to take control over who gains access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, Internet credit card transaction, or other services, including an extension of credit at point of sale.

When you place a security freeze on your credit report, within ten (10) business days you will be provided a personal identification number, password, or other equally or more secure method of authentication to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a specific party, parties, or period of time after the freeze is in place. To provide that authorization, you must contact the credit reporting agency and provide all of the following:

(1) The unique personal identification number or, password, or other method of authentication provided by the credit reporting agency;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the third party or parties who are to receive the credit report or the period of time for which the report shall be available to users of the credit report.

A credit reporting agency may not charge a fee to remove the freeze on your credit report or authorize the release of your credit report for a specific party, parties, or period of time after the freeze is in place.

Pursuant to § 6-48-5(a)(9), a credit reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze will not apply to "preauthorized approvals of credit."

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account, provided you have previously given your consent to this use of your credit reports. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a credit reporting agency or a user of your credit report.

(d) The information required to be disclosed by this section shall be disclosed in writing.

The information required to be disclosed pursuant to subsection (c) of this section shall be disclosed on one side of a separate document, with text no smaller than that prescribed by the Federal Trade Commission for the notice required under 15 U.S.C. § 1681g. The information required to be disclosed pursuant to subsection (c) of this section may accurately reflect changes in numerical items that change over time (such as the telephone number or address of Rhode Island state agencies), and remain in compliance.

(e) The director of the department of business regulation may revise this required notice by rule as appropriate from time to time so long as no new substantive rights are created therein.

6-48.1-8. Security freeze requirements.

(a)(1) A Rhode Island consumer may place a security freeze on their credit report. A credit reporting agency shall not charge a fee to Rhode Island consumers for placing or removing, removing for a specific party or parties, or removing for a specific period of time after the freeze is in place, a security freeze on a credit report.

(2) A consumer may place a security freeze on their credit report by making a request in writing by certified mail to a credit reporting agency.

(3) A security freeze shall prohibit, subject to the exceptions in this chapter and § 6-48-5, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

(4) This subsection does not prevent a credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

(b) A credit reporting agency shall place a security freeze on a consumer's credit report not later than five (5) business days after receiving a written request from the consumer.

(c) The credit reporting agency shall send a written confirmation of the security freeze to the consumer within ten (10) business days and shall provide the consumer with a unique personal identification number or password, other than the customer's social security number, or another method of authentication that is equally or more secure than a personal identification number (PIN) or password, to be used by the consumer when providing authorization for the release of their credit for a specific party, parties, or period of time.

(d) If the consumer authorizes their credit report to be accessed for a specific party, parties, or period of time while a freeze is in place, they shall contact the credit reporting agency, request that the freeze be temporarily lifted, and provide the following:

(1) Proper identification;

(2) The unique personal identification number or, password, or other method of authentication provided by the credit reporting agency pursuant to subsection (c) of this section;

and

(3) The proper information regarding the third party, parties, or time period for which the report shall be available to users of the credit report.

(e) A credit reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to lift temporarily a freeze on a credit report pursuant to subsection (d) of this section in an expedited manner.

(f) A credit reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report pursuant to subsection (d) of this section shall comply with the request not later than three (3) business days after receiving the request.

(g) A credit reporting agency shall remove or lift temporarily a freeze placed on a consumer's credit report only in the following cases:

(1) Upon consumer request, pursuant to subsection (d) or (j) of this section.

(2) If the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a credit reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this subsection, the credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(h) If a third party requests access to a credit report on which a security freeze is in effect and this request is in connection with an application for credit or any other use and the consumer does not allow their credit report to be accessed for that specific party or period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze pursuant to § 6-48-5, the credit reporting agency shall disclose to the consumer the process of placing and lifting temporarily a security freeze and the process for allowing access to information from the consumer's credit report for a specific party, parties, or period of time while the security freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A credit reporting agency shall remove a security freeze within three (3) business days of receiving a request for removal from the consumer who provides both of the following:

(1) Proper identification; and

(2) The unique personal identification number, password, or other method of authentication provided by the credit reporting agency pursuant to § 6-48-5.

(k) A credit reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

(l) The provisions of this section, including the security freeze, do not apply to the use of a consumer report by the following:

(1) A person, or the person's subsidiary, affiliate, agent, or assignee with which the consumer has or, prior to assignment, had an account, contract, or debtor-creditor relationship for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or debt, or extending credit to a consumer with a prior or existing account, contract, or debtor-creditor relationship. For purposes of this subsection, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection (d) of this section for purposes of facilitating the extension of credit or other permissible use.

(3) Any person acting pursuant to a court order, warrant, or subpoena.

(4) The office of child support services when investigating a child support case.

(5) The medical fraud and patient abuse unit of the department of the attorney general or its agents or assignee acting to investigate welfare or Medicaid fraud.

(6) The division of taxation, municipal taxing authorities, or the department of motor vehicles, or any of their agents or assignees, acting to investigate or collect delinquent taxes or assessments, including interest and penalties, unpaid court orders, or acting to fulfill any of their other statutory or charter responsibilities.

(7) A person's use of credit information for the purposes of prescreening as provided by the federal Fair Credit Reporting Act.

(8) Any person for the sole purpose of providing a credit file monitoring subscription service to which the consumer has subscribed.

(9) A credit reporting agency for the sole purpose of providing a consumer with a copy of their credit report upon the consumer's request.

(10) Any property and casualty insurance company for use in setting or adjusting a rate or underwriting for property and casualty insurance purposes.

6-48.1-9. One-stop freeze notification report.

(a) The director of the department of business regulation, in consultation with industry stakeholders, shall consider one or more methods to ease the burden on consumers when placing or lifting a credit security freeze, including the right to place a freeze with a single nationwide credit reporting agency and require that agency to initiate a freeze with other agencies.

(b) On or before January 15, 2022, the director of the department of business regulation

shall report their findings and recommendations to the governor, speaker of the house, and president of the senate.

6-48.1-10. Construction.

Nothing in this chapter shall be deemed to apply in any manner to any information or data that is subject to the Federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated under that act, or to information or data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA); provided, however, no entity or individual shall be exempt from the provisions of this chapter.

SECTION 2. This act shall take effect on January 1, 2021.

LC005062

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS -- ESTABLISHING THE "CONSUMER PERSONAL DATA PROTECTION ACT OF 2020"

***

This act would regulate data brokers. Data brokers would be required to annually register, to provide substantive notifications to consumers, and to adopt comprehensive data security programs.

This act would take effect on January 1, 2021.

LC005062