



101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

SB0240

Introduced 1/31/2019, by Sen. Michael E. Hastings

SYNOPSIS AS INTRODUCED:

New Act

Creates the Consumer Credit Reporting Agency Registration and Cybersecurity Program Act. Provides for requirements for consumer credit reporting agency registration. Contains provisions regarding grounds for revocation and suspension of a registration. Provides that by January 1, 2020, a consumer credit reporting agency must have a cybersecurity program documented in writing and designed to protect the confidentiality, integrity and availability of its information systems. Provides that a consumer credit reporting agency shall implement and maintain a written cybersecurity policy setting forth its policies and procedures for the protection of its information systems and nonpublic information stored on those information systems. Provides that a consumer credit reporting agency shall designate a qualified individual as a chief information security officer to oversee and implement its cybersecurity policy. Contains provisions concerning penetration testing and vulnerability assessments, audit trail, access privileges, and application security. Provides that a consumer credit reporting agency shall conduct periodic risk assessments of its information systems. Provides requirements for cybersecurity personnel and third-party service provider security policy. Provides that a consumer credit reporting agency shall establish a written incident response plan designed to promptly respond to a cybersecurity event. Provides that the consumer credit reporting agency shall notify the Department of Financial and Professional Regulation of the existence of a cybersecurity event no later than 72 hours after the event occurred. Makes other changes. Effective immediately.

LRB101 06790 JRG 51817 b

FISCAL NOTE ACT
MAY APPLY

A BILL FOR

1 AN ACT concerning regulation.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the
5 Consumer Credit Reporting Agency Registration and
6 Cybersecurity Program Act.

7 Section 5. Definitions. As used in this Act:

8 "Affiliate" means a person that controls, is controlled by,
9 or is under common control with another person.

10 "Authorized user" means any employee, contractor, agent or
11 other person that participates in the business operations of a
12 consumer credit reporting agency and is authorized to access
13 and use any information system and data of the consumer credit
14 reporting agency.

15 "Consumer" means an individual.

16 "Consumer report" means a written, oral, or other
17 communication of any information by a consumer reporting agency
18 bearing on a consumer's credit worthiness, credit standing,
19 credit capacity, character, general reputation, personal
20 characteristics, or mode of living that is used or expected to
21 be used or collected in whole or in part for the purpose of
22 serving as a factor in establishing the consumer's eligibility
23 for (i) credit or insurance to be used primarily for personal,

1 family, or household purposes, (ii) employment purposes, or
2 (iii) other purposes.

3 "Consumer reporting agency" means any person who, for
4 monetary fees, dues, or on a cooperative nonprofit basis,
5 regularly engages in whole or in part in the practice of
6 assembling or evaluating consumer credit information or other
7 information on consumers for the purpose of furnishing consumer
8 reports or investigative consumer reports to third parties.

9 "Consumer credit reporting agency" means a consumer
10 reporting agency that regularly engages in the practice of
11 assembling or evaluating and maintaining public record
12 information or credit account information from persons who
13 furnish that information regularly and in the ordinary course
14 of business for the purpose of furnishing consumer credit
15 reports to third parties bearing on a consumer's credit
16 worthiness, credit standing, and credit capacity.

17 "Cybersecurity event" means any act or attempt, successful
18 or unsuccessful, to gain unauthorized access to, disrupt, or
19 misuse an information system or information stored on such
20 information system.

21 "Department" means the Department of Financial and
22 Professional Responsibility.

23 "Financial institution" means a bank, savings bank,
24 savings and loan association, credit union, or any licensee
25 under the Consumer Installment Loan Act or the Sales Finance
26 Agency Act.

1 "Information system" means a discrete set of electronic
2 information resources organized for the collection,
3 processing, maintenance, use, sharing, dissemination or
4 disposition of electronic information, or any specialized
5 system such as industrial or process control systems, telephone
6 switching and private branch exchange systems, and
7 environmental control systems.

8 "Multi-factor authentication" means authentication through
9 verification of at least 2 of the following types of
10 authentication factors:

11 (1) knowledge factor, such as a password;

12 (2) possession factor, such as a token or text message
13 on a mobile phone; or

14 (3) inherence factor, such as a biometric
15 characteristic.

16 "Nonpublic information" means all electronic information
17 that is not publicly available information and is:

18 (1) business-related information of a consumer credit
19 reporting agency in which the tampering, or unauthorized
20 disclosure, access, or use of, would cause a material
21 adverse impact on the business, operations or security of
22 the consumer credit reporting agency;

23 (2) any information concerning an individual that
24 because of name, number, personal mark, or other identifier
25 can be used to identify such individual, in combination
26 with any one or more of the following data elements:

- 1 (i) social security number;
- 2 (ii) driver's license number or non-driver
3 identification card number;
- 4 (iii) account number, credit or debit card number;
- 5 (iv) any security code, access code or password
6 that would permit access to an individual's financial
7 account; or
- 8 (v) biometric records;
- 9 (3) any information or data, except age or gender, in
10 any form or medium created by or derived from a health care
11 provider or an individual that relates to:
- 12 (i) the past, present, or future physical, mental,
13 or behavioral health or condition of any individual or
14 a member of the individual's family;
- 15 (ii) the provision of health care to any
16 individual; or
- 17 (iii) payment for the provision of health care to
18 any individual.

19 "Penetration testing" means a test methodology in which
20 assessors attempt to circumvent or defeat the security features
21 of an information system by attempting penetration of databases
22 or controls from outside or inside the consumer credit
23 reporting agency's information systems.

24 "Person" means any individual or any non-governmental
25 entity, including, but not limited to, any non-governmental
26 partnership, corporation, branch, agency or association.

1 "Publicly available information" means any information
2 that a consumer credit reporting agency has a reasonable basis
3 to believe is lawfully made available to the general public
4 from federal, State, or local government records, widely
5 distributed media, or disclosures to the general public that
6 are required to be made by federal, State or local law.

7 (1) For the purposes of this Act, a consumer credit
8 reporting agency has a reasonable basis to believe that
9 information is lawfully made available to the general
10 public if the consumer credit reporting agency has taken
11 steps to determine:

12 (i) that the information is of the type that is
13 available to the general public; and

14 (ii) whether an individual can direct that
15 information to make it unavailable to the general
16 public and, if so, that such individual has not done
17 so.

18 "Risk assessment" means the risk assessment that each
19 consumer credit reporting agency is required to conduct under
20 Section 65.

21 "Risk-based authentication" means any risk-based system of
22 authentication that detects anomalies or changes in the normal
23 use patterns of a person and requires additional verification
24 of the person's identity when such deviations or changes are
25 detected, such as through the use of challenge questions.

26 "Senior officer" or "senior officers" means the senior

1 individual or individuals, acting collectively or as a
2 committee, responsible for the management, operations,
3 security, information systems, compliance or risk of a consumer
4 credit reporting agency, including a branch or agency of a
5 foreign banking organization subject to this Act.

6 "Third-party service provider" means a person that:

7 (1) is not an affiliate of the consumer credit
8 reporting agency;

9 (2) provides services to the consumer credit reporting
10 agency; and

11 (3) maintains, processes, or otherwise is permitted
12 access to nonpublic information through provision of
13 services to the consumer credit reporting agency.

14 Section 10. Registration.

15 (a) A consumer credit reporting agency that assembles,
16 evaluates, or maintains a consumer credit report on one or more
17 consumers located in the State of Illinois shall register with
18 the Department in a form and manner acceptable to the
19 Department.

20 (b) For a business entity, the officer or officers and
21 director or directors named in the registration application
22 shall be designated responsible for the business entity's
23 compliance with the financial services, banking, and insurance
24 laws, rules, and regulations of this State.

25 (c) A consumer credit reporting agency that assembles,

1 evaluates, or maintains a consumer credit report on any
2 consumer located in the State of Illinois at any time between
3 July 1, 2018 and September 1, 2019, shall make the registration
4 required by subsection (a) on or before September 1, 2019. Any
5 other consumer credit reporting agency shall make the
6 registration required by subsection (a) prior to assembling,
7 evaluating, or maintaining a consumer credit report on a
8 consumer located in the State of Illinois.

9 (d) A consumer credit reporting agency shall renew its
10 registration by January 1, 2020 for the 2020 calendar year, and
11 by January 1 of each successive year for the calendar year
12 thereafter.

13 (e) The Department may refuse to renew a consumer credit
14 reporting agency's registration if, in the Department's
15 judgment, the applicant or any member, principal, officer or
16 director of the applicant, is not trustworthy and is not
17 competent to act as or in connection with a consumer credit
18 reporting agency, or that any of the foregoing has given cause
19 for revocation or suspension of such registration, or has
20 failed to comply with any minimum standard.

21 (f) Registrants under this Section shall be subject to
22 examination by the Department as often as the Department may
23 deem it necessary. The Department may promulgate regulations
24 establishing methods and procedures for facilitating and
25 verifying compliance with the requirements of this Act and such
26 other regulations as necessary to enforce the provisions of

1 this Act.

2 Section 15. Acting without registration.

3 (a) No individual, firm, association, corporation or other
4 entity may assemble, evaluate, or maintain a consumer credit
5 report on any consumer located in the State of Illinois without
6 having a valid registration as a consumer credit reporting
7 agency filed as described in Section 10.

8 (b) No financial institution may pay any fee or other
9 compensation to any consumer credit reporting agency that is
10 required to be registered pursuant to Section 10 but fails to
11 possess the required registration.

12 (c) No regulated person may transmit any information about
13 a consumer located in the State of Illinois to a consumer
14 credit reporting agency that is required to be registered
15 pursuant to Section 10 but failed to possess the required
16 registration.

17 Section 20. Revocation and suspension of a registration.

18 (a) The Department may refuse to renew, revoke, or may
19 suspend the registration of a consumer credit report agency for
20 a period the Department determines if, after notice and
21 hearing, the Department determines that the registrant or any
22 member, principal, officer, director, or controlling person of
23 the registrant, has:

24 (1) violated any insurance, financial service, or

1 banking law or violated any regulation, subpoena or order
2 of the Department or any other State or federal agency with
3 authority to regulate consumer credit reporting agencies,
4 or has violated any law in the course of his or her
5 dealings in such capacity;

6 (2) provided materially incorrect, materially
7 misleading, materially incomplete or materially untrue
8 information in the registration application;

9 (3) failed to comply with the requirements of this Act,
10 including, but not limited to, Sections 30 through 105
11 concerning cybersecurity;

12 (4) used fraudulent, coercive or dishonest practices;
13 demonstrated incompetence; demonstrated untrustworthiness;
14 or demonstrated financial irresponsibility in the conduct
15 of business in this state or elsewhere;

16 (5) improperly withheld, misappropriated or converted
17 any moneys or properties received in the course of business
18 in this State or elsewhere;

19 (6) has been convicted of a felony;

20 (7) admitted or has been found to have committed any
21 unfair trade practice or fraud;

22 (8) had a consumer credit reporting agency
23 registration or its equivalent, denied, suspended, or
24 revoked in any other state, province, district or
25 territory; or

26 (9) failed to pay state income tax or comply with any

1 administrative or court order directing payment of state
2 income tax.

3 (b) Before revoking or suspending the registration of any
4 consumer credit reporting agency pursuant to this Act, the
5 Department shall give notice to the registrant and shall hold,
6 or cause to be held, a hearing not less than 10 days after the
7 giving of such notice.

8 (c) If a registration pursuant to this Act is revoked or
9 suspended by the Department, then the Department shall
10 forthwith give notice to the registrant.

11 (d) The revocation or suspension of any registration
12 pursuant to this Act shall terminate forthwith such
13 registration.

14 Section 25. Prohibited practices. No consumer credit
15 reporting agency that assembles, evaluates, or maintains a
16 consumer credit report on any consumer located in the State of
17 Illinois shall:

18 (1) Directly or indirectly employ any scheme, device or
19 artifice to defraud or mislead a consumer.

20 (2) Engage in any unfair, deceptive, or predatory act or
21 practice toward any consumer, or misrepresent or omit any
22 material information in connection with the assembly,
23 evaluation, or maintenance of a credit report for a consumer
24 located in the State of Illinois.

25 (3) Engage in any unfair, deceptive, or abusive act or

1 practice in violation of Section 1036 of the Dodd-Frank Wall
2 Street Reform and Consumer Protection Act.

3 (4) Include inaccurate information in any consumer report
4 relating to a consumer located in the State of Illinois.

5 (5) Refuse to communicate with an authorized
6 representative of a consumer located in the State of Illinois
7 who provides a written authorization signed by the consumer,
8 provided that the consumer credit reporting agency may adopt
9 procedures reasonably related to verify that the
10 representative is in fact authorized to act on behalf of the
11 consumer.

12 (6) Make any false statement or make any omission of a
13 material fact in connection with any information or reports
14 filed with a governmental agency or in connection with any
15 investigation conducted by another governmental agency.

16 Section 30. Cybersecurity program.

17 (a) By January 1, 2020, a consumer credit reporting agency
18 that assembles, evaluates, or maintains a consumer credit
19 report on Illinois consumers must have in place a written
20 cybersecurity program designed to protect the confidentiality,
21 integrity and availability of the consumer credit reporting
22 agency's information systems.

23 (b) The cybersecurity program shall be based on the
24 consumer credit reporting agency's risk assessment and
25 designed to perform the following core cybersecurity

1 functions:

2 (1) identify and assess internal and external
3 cybersecurity risks that may threaten the security or
4 integrity of nonpublic information stored on the consumer
5 credit reporting agency's information systems;

6 (2) use defensive infrastructure and the
7 implementation of policies and procedures to protect the
8 consumer credit reporting agency's information systems,
9 and the nonpublic information stored on those information
10 systems, from unauthorized access, use, or other malicious
11 acts;

12 (3) detect cybersecurity events;

13 (4) respond to identified or detected cybersecurity
14 events to mitigate any negative effects;

15 (5) recover from cybersecurity events and restore
16 normal operations and services; and

17 (6) fulfill applicable regulatory reporting
18 obligations.

19 (c) A consumer credit reporting agency may meet the
20 requirements of this Act by adopting relevant and applicable
21 provisions of a cybersecurity program maintained by an
22 affiliate, provided that such provisions satisfy the
23 requirements of this Act, as applicable to the consumer credit
24 reporting agency.

25 (d) All documentation and information relevant to the
26 consumer credit reporting agency's cybersecurity program shall

1 be made available to the Department upon request.

2 Section 35. Cybersecurity policy. Each consumer credit
3 reporting agency shall implement and maintain a written policy
4 or policies, approved by a senior officer, the consumer credit
5 reporting agency's board of directors, an appropriate
6 committee thereof, or equivalent governing body, setting forth
7 the consumer credit reporting agency's policies and procedures
8 for the protection of its information systems and nonpublic
9 information stored on those information systems. The
10 cybersecurity policy shall be based on the consumer credit
11 reporting agency's risk assessment and address the following
12 areas to the extent applicable to the consumer credit reporting
13 agency's operations:

- 14 (1) information security;
- 15 (2) data governance and classification;
- 16 (3) asset inventory and device management;
- 17 (4) access controls and identity management;
- 18 (5) business continuity and disaster recovery planning
19 and resources;
- 20 (6) systems operations and availability concerns;
- 21 (7) systems and network security;
- 22 (8) systems and network monitoring;
- 23 (9) systems and application development and quality
24 assurance;
- 25 (10) physical security and environmental controls;

- 1 (11) consumer data privacy;
- 2 (12) vendor and third-party service provider
- 3 management;
- 4 (13) risk assessment; and
- 5 (14) incident response.

6 Section 40. Chief information officer.

7 (a) A consumer credit reporting agency shall designate a
8 qualified individual responsible for overseeing and
9 implementing the consumer credit reporting agency's
10 cybersecurity program and enforcing its cybersecurity policy.
11 The chief information security officer may be employed by the
12 consumer credit reporting agency, one of its affiliates, or a
13 third-party service provider. To the extent this requirement is
14 met using a third-party service provider or an affiliate, the
15 consumer credit reporting agency shall:

16 (1) retain responsibility for compliance with this
17 Act;

18 (2) designate a senior member of the consumer credit
19 reporting agency's personnel responsible for direction and
20 oversight of the third-party service provider; and

21 (3) require the third-party service provider to
22 maintain a cybersecurity program that protects the
23 consumer credit reporting agency in accordance with the
24 requirements of this Act.

25 (b) The chief information security officer of each consumer

1 credit reporting agency shall report in writing at least
2 annually to the consumer credit reporting agency's board of
3 directors or equivalent governing body. If no such board of
4 directors or equivalent governing body exists, such report
5 shall be timely presented to a senior officer of the consumer
6 credit reporting agency responsible for the consumer credit
7 reporting agency's cybersecurity program. The chief
8 information security officer shall report on the consumer
9 credit reporting agency's cybersecurity program and material
10 cybersecurity risks. The chief information security officer
11 shall consider to the extent applicable:

12 (1) the confidentiality of nonpublic information and
13 the integrity and security of the consumer credit reporting
14 agency's information systems;

15 (2) the consumer credit reporting agency's
16 cybersecurity policies and procedures;

17 (3) material cybersecurity risks to the consumer
18 credit reporting agency;

19 (4) overall effectiveness of the consumer credit
20 reporting agency's cybersecurity program; and

21 (5) material cybersecurity events involving the
22 consumer credit reporting agency during the time period
23 addressed by the report.

24 Section 45. Penetration testing and vulnerability
25 assessments. The cybersecurity program for a consumer credit

1 reporting agency shall include monitoring and testing,
2 developed in accordance with the consumer credit reporting
3 agency's risk assessment, designed to assess the effectiveness
4 of the consumer credit reporting agency's cybersecurity
5 program. The monitoring and testing shall include continuous
6 monitoring or periodic penetration testing and vulnerability
7 assessments. Absent effective continuous monitoring or other
8 systems to detect, on an ongoing basis, changes in information
9 systems that may create or indicate vulnerabilities, consumer
10 credit agencies shall conduct:

11 (1) annual penetration testing of the consumer credit
12 reporting agency's information systems determined each
13 given year based on relevant identified risks in accordance
14 with the risk assessment; and

15 (2) vulnerability assessments every 2 years, including
16 any systematic scans or reviews of information systems
17 reasonably designed to identify publicly known
18 cybersecurity vulnerabilities in the consumer credit
19 reporting agency's information systems based on the risk
20 assessment.

21 Section 50. Audit trail.

22 (a) Each consumer credit reporting agency shall securely
23 maintain systems that, to the extent applicable and based on
24 its risk assessment:

25 (1) are designed to reconstruct material financial

1 transactions sufficient to support normal operations and
2 obligations of the consumer credit reporting agency; and

3 (2) include audit trails designed to detect and respond
4 to cybersecurity events that have a reasonable likelihood
5 of materially harming any material part of the normal
6 operations of the consumer credit reporting agency.

7 (b) Each consumer credit reporting agency shall maintain
8 records required by paragraph (1) of subsection (a) for not
9 fewer than 5 years and shall maintain records required by
10 paragraph (2) of subsection (a) for not fewer than 3 years.

11 Section 55. Access privileges. As part of its cybersecurity
12 program, based on the consumer credit reporting agency's risk
13 assessment, a consumer credit reporting agency shall limit user
14 access privileges to information systems that provide access to
15 nonpublic information and shall periodically review such
16 access privileges.

17 Section 60. Application security.

18 (a) A consumer credit reporting agency's cybersecurity
19 program shall include written procedures, guidelines, and
20 standards designed to ensure the use of secure development
21 practices for in-house developed applications utilized by the
22 consumer credit reporting agency, and procedures for
23 evaluating, assessing, or testing the security of externally
24 developed applications utilized by the consumer credit

1 reporting agency within the context of the consumer credit
2 reporting agency's technology environment.

3 (b) All such procedures, guidelines, and standards shall be
4 periodically reviewed, assessed and updated as necessary by the
5 chief information security officer or a qualified designee of
6 the consumer credit reporting agency.

7 Section 65. Risk assessment.

8 (a) A consumer credit reporting agency shall conduct a
9 periodic risk assessment of the consumer credit reporting
10 agency's information systems sufficient to inform the designer
11 of the cybersecurity program as required by this Act. Such risk
12 assessment shall be updated as reasonably necessary to address
13 changes to the consumer credit reporting agency's information
14 systems, nonpublic information or business operations. The
15 consumer credit reporting agency's risk assessment shall allow
16 revision of controls to respond to technological developments
17 and evolving threats and shall consider the particular risks of
18 the consumer credit reporting agency's business operations
19 related to cybersecurity, nonpublic information collected or
20 stored, information systems utilized, and the availability and
21 effectiveness of controls to protect nonpublic information and
22 information systems.

23 (b) The risk assessment shall be carried out in accordance
24 with written policies and procedures and shall be documented.
25 Such policies and procedures shall include:

1 (1) criteria for the evaluation and categorization of
2 identified cybersecurity risks or threats facing the
3 consumer credit reporting agency;

4 (2) criteria for the assessment of the
5 confidentiality, integrity, security and availability of
6 the consumer credit reporting agency's information systems
7 and nonpublic information, including the adequacy of
8 existing controls in the context of identified risks; and

9 (3) requirements describing how identified risks will
10 be mitigated or accepted based on the risk assessment and
11 how the cybersecurity program will address the risks.

12 Section 70. Cybersecurity personnel and intelligence.

13 (a) In addition to the requirements set forth in Section
14 40, a consumer credit reporting agency shall:

15 (1) utilize qualified cybersecurity personnel of the
16 consumer credit reporting agency, an affiliate, or a
17 third-party service provider sufficient to manage the
18 consumer credit reporting agency's cybersecurity risks and
19 to perform or oversee the performance of the core
20 cybersecurity functions specified in paragraphs (1)
21 through (6) of subsection (b) of Section 30;

22 (2) provide cybersecurity personnel with cybersecurity
23 updates and training sufficient to address relevant
24 cybersecurity risks; and

25 (3) verify that key cybersecurity personnel take steps

1 to maintain current knowledge of changing cybersecurity
2 threats and countermeasures.

3 (b) A consumer credit reporting agency may choose to
4 utilize an affiliate or qualified third-party service provider
5 to assist in complying with the requirements set forth in this
6 Act, subject to the requirements set forth in Section 75.

7 Section 75. Third-party service provider security policy.

8 (a) Each consumer credit reporting agency shall implement
9 written policies and procedures designed to ensure the security
10 of information systems and nonpublic information that are
11 accessible to, or held by, third-party service providers. Such
12 policies and procedures shall be based on the risk assessment
13 of the consumer credit reporting agency and shall address to
14 the extent applicable:

15 (1) The identification and risk assessment of
16 third-party service providers.

17 (2) Minimum cybersecurity practices required to be met
18 by such third-party service providers in order for them to
19 do business with the consumer credit reporting agency.

20 (3) Due diligence processes used to evaluate the
21 adequacy of cybersecurity practices of such third-party
22 service providers.

23 (4) Periodic assessment of such third-party service
24 providers based on the risk they present and the continued
25 adequacy of their cybersecurity practices.

1 (b) Such policies and procedures shall include relevant
2 guidelines for due diligence or contractual protections
3 relating to third-party service providers to the extent
4 applicable addressing:

5 (1) the third-party service provider's policies and
6 procedures for access controls, including its use of
7 multi-factor authentication as required by Section 80 of
8 this Act, to limit access to relevant information systems
9 and nonpublic information;

10 (2) the third-party service provider's policies and
11 procedures for use of encryption as required by Section 95
12 to protect nonpublic information in transit and at rest;

13 (3) notice to be provided to the consumer credit
14 reporting agency in the event of a cybersecurity event
15 directly impacting the consumer credit reporting agency's
16 information systems or the consumer credit reporting
17 agency's nonpublic information being held by the
18 third-party service provider; and

19 (4) representations and warranties addressing the
20 third-party service provider's cybersecurity policies and
21 procedures that relate to the security of the consumer
22 credit reporting agency's information systems or nonpublic
23 information.

24 Section 80. Multi-factor authentication.

25 (a) Based on its risk assessment, each consumer credit

1 reporting agency shall use effective controls, which may
2 include multi-factor authentication or risk-based
3 authentication, to protect against unauthorized access to
4 nonpublic information or information systems.

5 (b) Multi-factor authentication shall be utilized for any
6 individual accessing the consumer credit reporting agency's
7 internal networks from an external network, unless the consumer
8 credit reporting agency's chief information security officer
9 has approved in writing the use of reasonably equivalent or
10 more secure access controls.

11 Section 85. Limitations on data retention. As part of its
12 cybersecurity program, a consumer credit reporting agency
13 shall include policies and procedures for the secure disposal
14 on a periodic basis of any nonpublic information that is no
15 longer necessary for business operations or for other
16 legitimate business purposes of the consumer credit reporting
17 agency, except where such information is otherwise required to
18 be retained by law or regulation, or where targeted disposal is
19 not reasonably feasible due to the manner in which the
20 information is maintained.

21 Section 90. Training and monitoring. As part of its
22 cybersecurity program, each consumer credit reporting agency
23 shall:

24 (1) implement risk-based policies, procedures and

1 controls designed to monitor the activity of authorized
2 users and detect unauthorized access or use of, or
3 tampering with, nonpublic information by such authorized
4 users; and

5 (2) provide regular cybersecurity awareness training
6 to all personnel that is updated to reflect risks
7 identified by the consumer credit reporting agency in its
8 risk assessment.

9 Section 95. Encryption of nonpublic information.

10 (a) As part of its cybersecurity program, based on its risk
11 assessment, each consumer credit reporting agency shall
12 implement controls, including encryption, to protect nonpublic
13 information held or transmitted by the consumer credit
14 reporting agency both in transit over external networks and at
15 rest.

16 (1) To the extent a consumer credit reporting agency
17 determines that encryption of nonpublic information in
18 transit over external networks is infeasible, the consumer
19 credit reporting agency may instead secure such nonpublic
20 information using effective alternative compensating
21 controls reviewed and approved by the consumer credit
22 reporting agency's chief information security officer.

23 (2) To the extent a consumer credit reporting agency
24 determines that encryption of nonpublic information at
25 rest is infeasible, the consumer credit reporting agency

1 (4) external and internal communications and
2 information sharing;

3 (5) identification of requirements for the remediation
4 of any identified weaknesses in information systems and
5 associated controls;

6 (6) documentation and reporting regarding
7 cybersecurity events and related incident response
8 activities; and

9 (7) the evaluation and revision as necessary of the
10 incident response plan following a cybersecurity event.

11 Section 105. Notice to the Department.

12 (a) A consumer credit reporting agency shall notify the
13 Department as promptly as possible but in no event later than
14 72 hours from a determination that a cybersecurity event has
15 occurred that is either of the following:

16 (1) cybersecurity events impacting the consumer credit
17 reporting agency of which notice is required to be provided
18 to a government body, self-regulatory agency or any other
19 supervisory body; or

20 (2) cybersecurity events that have a reasonable
21 likelihood of materially harming any material part of the
22 normal operation of the consumer credit reporting agency.

23 (b) A consumer credit reporting agency shall submit to the
24 Department a written statement annually covering the prior
25 calendar year. This statement shall be submitted by February

1 15th in such manner as determined acceptable by the Department,
2 certifying that the consumer credit reporting agency is in
3 compliance with the requirements set forth in this Act. Each
4 consumer credit reporting agency shall maintain all records,
5 schedules, and data supporting this certificate for a period of
6 5 years for examination purposes conducted by the Department.
7 To the extent a consumer credit reporting agency has identified
8 areas, systems or processes that require material improvement,
9 updating or redesign, the consumer credit reporting agency
10 shall document the identification and the remedial efforts
11 planned and underway to address such areas, systems or
12 processes. Such documentation must be available for inspection
13 by the Department.

14 Section 110. Enforcement. This Act shall be enforced by the
15 Department pursuant to, and is not intended to limit, the
16 Department's authority under any applicable laws.

17 Section 115. Severability. If any provision of this Act or
18 the application thereof to any person or circumstance is
19 adjudged invalid by a court of competent jurisdiction, such
20 judgment shall not affect or impair the validity of the other
21 provisions of this Act or the application thereof to other
22 persons or circumstances.

23 Section 999. Effective date. This Act takes effect upon
24 becoming law.