Bloomberg Law®

Domestic Privacy Profile: Minnesota

Prepared in cooperation with

Melissa Krasnow

Partner, VLP Law Group LLP, Minneapolis

Bloomberg Law
Privacy & Data Security

Domestic Privacy Profile: MINNESOTA

Melissa Krasnow, Partner, VLP Law Group, LLP, Minneapolis, provided expert review of the Minnesota Profile and wrote the Risk Environment Section. [Last updated December 2018. – Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

Minn. Const. art. I, § 10 protects the right of people to be "secure in their persons, houses, papers, and effects against unreasonable searches and seizures." Besides this general provision, our research has uncovered no data-specific privacy provisions in the Minnesota Constitution.

B. PERSONAL DATA PROTECTION PROVISIONS

1. Who is covered?

Minnesota law contains two data breach notification provisions, one applying to private information holders (Minn. Stat. § 325E.61(1)(a) to Minn. Stat. § 325E.61(1)(b)), and the other applying to the government (Minn. Stat. § 13.055). Under these data breach notification provisions, information holders are required to notify Minnesota residents or any owner or licensee of personal information whose information "was, or is reasonably believed to have been, acquired by an unauthorized person" (Minn. Stat. § 325E.61), whereas the government is required to notify "any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person" (Minn. Stat. § 13.055(2)(a)).

Other data protection provisions apply to:

- victims of domestic violence, sexual assault, or stalking (Minn. Stat. § 5B.02(e));
- subjects of consumer reports (Minn. Stat. § 13C.016);
- individuals about whom a government agency has collected or maintained data where the individual "is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual." (Minn. Stat. § 13.02(5));
- customers of financial institutions (Minn. Stat. § 47.69);
- consumers who pay service providers for access to the internet (Minn. Stat. § 325M.01(2));
- renters, purchasers, or subscribers of goods or services from a videotape service provider or seller (Minn. Stat. § 325I.01(2));
- individuals with a past, present, or proposed relationship to an insurance policy (Minn. Stat. § 72A.491(11));
- natural persons who have received health care services from a provider for treatment or examination of a medical, psychiatric, or mental condition, the surviving spouse and parents of such deceased patient, or the representative thereof (Minn. Stat. § 144.291(2)(g));

- applicants for drivers' licenses (Minn. Stat. § 171.12); and
- employees (Minn. Stat. § 181.950(6)).

2. What is covered?

A number of Minnesota provisions provide specific protections for personal information. Minnesota's breach notification law, for one, defines "personal information" as an individual's first name or first initial and last name, in combination with a social security number; a driver's license number or Minnesota identification card number; or an account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account (Minn. Stat. § 325E.61(1)(e)). However, publicly available information that is lawfully made available to the general public from federal, state, or local government records is not covered (Minn. Stat. § 325E.61(1)(f)).

In addition, the Minnesota Insurance Fair Information Reporting Act defines "personal information" as "individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics," including name, address, and health record information, and subject to certain exclusions (Minn. Stat. § 72A.491(17)).

Restrictions on internet service providers' information practices further define "personally identifiable information" as information that identifies a specific consumer's physical address, electronic address, or telephone; records of specific materials or services requested or maintained from an internet service provider, internet or online site visited, or any contents of the consumer's data storage devices (Minn. Stat. § 325M.01(5)).

Finally, Minnesota's protections for customers of videotape services define "personally identifiable information" as "information that identifies a person as having requested or obtained specific video materials or services from a videotape service provider or videotape seller" (Minn. Stat. § 325I.01(3)).

Other provisions of Minnesota law provide protections for the following:

- identity, including any name, number, or transmission that may be used to identify a specific individual or entity (Minn. Stat. § 609.527(1)(d));
- the residential, school, and work addresses of certified participants of Minnesota's victim protection program (Minn. Stat. § 5B.02(b));
- data maintained by the government "in which any individual is or can be identified as the subject," unless identifying data is "only incidental to the data and the data are not accessed by the name or other identifying data of any individual" (Minn. Stat. § 13.02(5));
- data relating to an individual maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student (Minn. Stat. § 13.32(1)(a));
- data in individuals created, collected, received, or maintained by the Department of Health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation necessary for the public health (Minn. Stat. § 13.3805(1)(a)(2));
- consumer reports (Minn. Stat. § 13C.001(3));
- information related to transfers of electronic funds (Minn. Stat. § 47.69);
- information relating to the past, present, or future physical or mental health or condition of a patient, provision of care to a patient, or payment for such care (Minn. Stat. § 144.291);
- drug and alcohol tests (Minn. Stat. § 181.950(5));
- genetic tests (Minn. Stat. § 181.974(1)(a));

- information concerning the geographical location of a telecommunications device (Minn. Stat. § 237.82(2));
- records relating to drivers' license applications (Minn. Stat. § 171.12); and
- electronic communications, including "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system" (Minn. Stat. § 626A.01(14)).

3. Who must comply?

Minnesota's breach notification law applies to persons or businesses conducting business in Minnesota who own or license data that includes personal information (Minn. Stat. § 325E.61(1)(a)), as well as persons or businesses who maintain data containing personal information that the person or business does not own (Minn. Stat. § 325E.61(1)(b)).

Other data protection provisions apply to:

- government entities (Minn. Stat. § 13.01(3); Minn. Stat. § 13.3805(1); Minn. Stat. § 171.12);
- public educational agencies or institutions or a person acting therefor (Minn. Stat. § 13.32);
- the Minnesota Secretary of State (Minn. Stat. § 5B.07);
- consumer reporting agencies (Minn. Stat. § 13C.001(4));
- financial institutions (Minn. Stat. § 47.61(4));
- insurers (Minn. Stat. § 72A.491);
- health care service providers (Minn. Stat. § 144.291(2)(i));
- employers (Minn. Stat. § 181.974(1)(b));
- drug and alcohol testing laboratories (Minn. Stat. § 181.954);
- internet service providers (Minn. Stat. § 325M.01(3));
- landlords (Minn. Stat. § 5B.10);
- natural persons and certain entities subject to Minnesota's consumer fraud provisions (Minn. Stat. § 325F.68(3)); and
- videotape sellers and service providers (Minn. Stat. § 325I.01(4); Minn. Stat. § 325I.01(5)).

C. Data Management Provisions

1. Notice & Consent

Our research has not uncovered any generally applicable notice requirements in Minnesota. However, Minnesota law requires health care service providers to provide patients with a written notice concerning practices and rights with respect to access to health records. The notice must explain that disclosures of health records may be made without the written consent of the patient and that the patient maintains the right to access and obtain copies of the patient's health records and other information about the patient that is maintained by the provider (Minn. Stat. § 144.292(4)).

2. Collection & Use

Government data collection: Government entities may only collect, store, use, or disseminate an individual's private or confidential data for the purposes given to the individual at the time of collection, unless an exception applies. Exceptions include the following:

- data collected before Aug. 1, 1975, that has not been treated as public data, may be used, stored, and disseminated for the purposes for which the data was originally collected or for purposes which are specifically approved by the commissioner of the Department of Administration as necessary to public health, safety, or welfare;

- private or confidential data may be used and disseminated to individuals or entities specifically authorized access to that data by state, local, or federal law enacted or promulgated after the collection of the data;
- private or confidential data may be used and disseminated to individuals or entities subsequent to the collection of the data when the responsible authority maintaining the data has requested approval for a new or different use or dissemination of the data and that request has been specifically approved by the commissioner as necessary to carry out a function assigned by law;
- private data may be used by and disseminated to any person or entity if the individual subject or subjects of the data have given their informed consent; and
- private or confidential data on an individual may be discussed at a meeting open to the public (Minn. Stat. § 13.05(4)).

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)). If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, the person or entity is liable to any affected card issuers for resulting costs (Minn. Stat. § 325E.64(3)).

3. Disclosure to Third Parties

Data protection for victims of violence: Disclosing address information of victims of violence who are enrolled in a data protection program is prohibited (Minn. Stat. § 5B.07), as is the display of a participant's name at a protected address by a landlord (Minn. Stat. § 5B.10). For more information see Section I.D.13.

Educational data held by public institutions: Any data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution that relates to a student may not be disclosed, except pursuant to court order, pursuant to specific authorization by statute and pursuant to certain other specified exceptions (Minn. Stat. § 13.32(3)).

Employee alcohol & drug test results: Test result reports and other information acquired in the drug or alcohol testing process are considered private and confidential information with respect to private sector employees and job applicants and private data on individuals with respect to public sector employees and job applicants. Such data may not be disclosed by an employer or laboratory to another employer or to a third-party individual, governmental agency, or private organization without the written consent of the employee or job applicant tested (Minn. Stat. § 181.954(2)).

Internet service providers: Internet service providers are prohibited from knowingly disclosing personally identifiable information of their customers, subject to certain exceptions (Minn. Stat. § 325M.02). Exceptions permit disclosure upon subpoena, to law enforcement, by court order or warrant, to court in a civil action, to the customer by request, when incidental to the internet service provider's ordinary course of business, to other internet service providers for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the internet service provider or with the authorization of the consumer (Minn. Stat. § 325M.03; Minn. Stat. § 325M.04(1)).

Remedies: A consumer who prevails or substantially prevails in an action is entitled to recover the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded (Minn. Stat. § 325M.07).

Insurance and health provisions: An insurer, insurance agent, or insurance-support organization must not disclose any personal or privileged information about a person collected or received in connection with an insurance transaction without the authorization of that person, subject to certain exceptions (Minn. Stat. § 72A.502(1); see Section I.E.7.). In addition, provisions of Minnesota law governing specific types of health care service providers prohibit disclosure of a patient's health records to a person without a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release, specific authorization by law, or a representation from a provider that holds a signed and dated consent from the patient authorizing the release (Minn. Stat. § 144.293(2); see Section I.D.9.).

Videotape sellers and service providers: Videotape sellers and service providers are prohibited from knowingly disclosing personally identifiable information of any customer to any person, unless required by subpoena, court order in a civil proceeding, or law enforcement pursuant to warrant (Minn. Stat. § 325I.02(1) to Minn. Stat. § 325I.02(2)).

Credit reports: If a security freeze is placed on a consumer's credit report, consumer reporting agencies are prohibited from releasing information in the consumer's consumer report to a third party in connection with the extension of credit or the opening of an account without prior express authorization from the consumer (Minn. Stat. § 13C.016(1)(b)).

4. Data Storage

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)).

Remedies: If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, that person or entity is required to reimburse the financial institution that issued any cards affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The financial institution may also recover costs for damages paid to cardholders injured by the breach (Minn. Stat. § 325E.64(3)).

5. Access & Correction

Access to health records: The Minnesota code contains multiple provisions that define patients' rights to access health records held by both insurers and health care service providers.

Insurer: Upon receiving a written request from an individual for access to personal information about the individual, an insurer, insurance agent, or insurance-support organization must inform the individual of the nature and substance of the personal information, including health information, that they possess; permit the individual to see and copy, in person, the personal information; permit the individual to obtain by mail a copy of all of the personal information or a reasonably described portion thereof; disclose to the individual the identity of those persons to whom the insurer, insurance agent, or insurance-support organization has disclosed the personal information within two years before the request; and provide the individual with a summary of the procedures by which the person may request correction, amendment, or deletion of personal information (Minn. Stat. § 72A.497(1); Minn. Stat. § 72A.497(3)).

Health care service providers: Upon request, a health care service provider must provide complete and current information it possesses concerning the patient's diagnosis, treatment, and prognosis (Minn. Stat. § 144.292(2)). In addition, upon a patient's written request, a health care service

provider must make available to the patient copies of the patient's health record at a reasonable cost (Minn. Stat. § 144.292(5)). However, if a health care service provider reasonably determines that the information is detrimental to the physical or mental health of the patient or is likely to cause the patient to inflict self-harm or to harm another, the health care service provider may withhold the information from the patient and may supply the information to an appropriate third party or to another provider (Minn. Stat. § 144.292(7)(a)).

Student access to private records restricted: Students do not have the right of access to private data as to financial records and statements of the students' parents or any information therein (Minn. Stat. § 13.32(4)).

6. Data Security

Government data security: The state official designated as the responsible authority must establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that is not public is only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure as well as establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected, and develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law (Minn. Stat. § 13.05(5)(a)). In addition, at least once a year, each government entity is required to conduct a comprehensive security assessment of any personal information it maintains (Minn. Stat. § 13.055(6)).

Internet service providers: Internet service providers must take reasonable steps to maintain the security and privacy of consumers' personally identifiable information (Minn. Stat. § 325M.05).

Remedies: A consumer who prevails or substantially prevails in an action is entitled to recover the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded (Minn. Stat. § 325M.07).

Driver information services: Minnesota law requires the Commissioner of Public Safety to "establish written procedures to ensure that only individuals authorized by law may enter, update, or access not public data collected, created, or maintained by the driver and vehicle services information system," to revoke the authorization of anyone who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law, and to arrange an independent biennial audit of the information system to determine whether data are classified correctly, how data are used and for verifying compliance (Minn. Stat. § 171.12(1a)).

7. Data Disposal

Government data disposal: When disposing of not public data, the data must be destroyed in a way that prevents its contents from being determined (Minn. Stat. § 13.05(5)(b)).

8. Data Breach

Minn. Stat. § 325E.61(1)(a) provides that following discovery of a breach of the security of the system, "any person or business that conducts business in" Minnesota that owns or maintains data including personal information must notify any Minnesota residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Minn. Stat. § 325E.61(b) further requires any person or business who maintains data including personal information, but does not own or license such information, to notify the owner or licensee immediately following discovery of a breach.

Primary definitions: A "breach of the security of the system" is an means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information, not including good faith acquisition by an employee or agent for the purposes of the person or business without further use or unauthorized disclosure (Minn. Stat. § 325E.61(d)).

"Personal information" is an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

- social security number;
- driver's license number or Minnesota identification card number; or
- account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account (Minn. Stat. § 325E.61(1)(e)).

The term does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records (Minn. Stat. § 325E.61(1)(f)).

Form and content of notice: Minnesota law permits persons or businesses that conduct business in Minnesota to provide notice of a breach of the security of the system by written notice, electronic notice, or substitute notice. Substitute notice is permitted if the information holder demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 persons, or the information holder does not have sufficient contact information (Minn. Stat. § 325E.61(1)(g)).

Notice to nationwide consumer reporting agencies: If providing notice would require notification of more than 500 persons at one time, the person providing notice must also notify any consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, within 48 hours, of the timing, distribution, and content of the notices (Minn. Stat. § 325E.61(2)).

Exceptions to requirements: If a person or business maintains its own information security policy that includes notification procedures consistent with the timing requirements of the general Minnesota data breach notification law, it will be considered in compliance with the notification requirements of the data breach notification law (Minn. Stat. § 325E.61(1)(h)). In addition, the breach notification requirements do not apply to any "financial institution" as defined by the federal Gramm-Leach-Bliley Act, 15 U.S.C. § 6809(3) (Minn. Stat. § 325E.61(4)).

Government data breach: Minn. Stat. § 13.055 imposes data breach notification requirements for Minnesota state government.

Primary definitions (government): A "breach of the security of the data" is any "unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data." However, the definition does not cover good faith acquisition or access by an employee, contractor, or agent of a government entity if the government data is not provided to, viewable by an unauthorized person or accessed for a purpose not described in the procedures required by Minn. Stat. § 13.05(5) " (Minn. Stat. § 13.055(1)(a)).

"Contact information" means "either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by the government entity" (Minn. Stat. § 13.055(1)(b)).

Form and content of notice (government): A government entity that collects, creates, receives, maintains, or disseminates private or confidential information on individuals must disclose any

breach of the security to any individual whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay (Minn. Stat. § 13.055(2)(a)). The government entity may provide written notice, electronic notice, or substitute notice, if the government entity demonstrates that the cost of providing written notice would exceed $250,000, the affected class of individuals to be notified exceeds 500,000, or the government entity does not have sufficient contact information (Minn. Stat. § 13.055(4)).

Government notice to nationwide consumer reporting agencies: If providing notice would require notification of more than 1,000 individuals at one time, the government entity must also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices (Minn. Stat. § 13.055(5)(a)).

Data security: At least once a year, each government entity is required to conduct a comprehensive security assessment of any personal information it maintains (Minn. Stat. § 13.055(6)).

Remedies: A government entity that violates the data breach notification requirements for Minnesota state government is liable to a person or representative of a decedent who suffers any damage as a result of the violation. For a willful violation, the government entity in addition is liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation (Minn. Stat. § 13.08(1)). A government entity that violates or proposes to violate these requirements may be enjoined by the district court (Minn. Stat. § 13.08(2)). An action to compel compliance may be brought (Minn. Stat. § 13.08(4)). In addition, there are administrative penalties (Minn. Stat. § 13.085) and criminal penalties (Minn. Stat. § 13.09).

9. Data Transfer & Cloud Computing

Our research has revealed no generally applicable data transfer or cloud computing provisions in Minnesota. However, the Minnesota State Bar Association has published guidance on cloud computing for lawyers considering a cloud-based service.

10. Other Provisions

Our research has revealed no other generally applicable data management provisions in Minnesota.

D. SPECIFIC TYPES OF DATA

1. Biometric Data

Our research has revealed no provisions specifically applicable to biometric data in Minnesota.

2. Consumer Data

Videotape sellers and service providers: Videotape sellers and service providers are prohibited from knowingly disclosing personally identifiable information of any customer to any person, unless required by subpoena, court order in a civil proceeding or law enforcement pursuant to warrant (Minn. Stat. § 325I.02(1) to Minn. Stat. § 325I.02(2)).

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)).

Remedies: If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, that person or entity is required to reimburse the financial institution that issued any cards affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The financial institution may also recover costs for damages paid to cardholders injured by the breach (Minn. Stat. § 325E.64(3)).

Internet service providers: Internet service providers must take reasonable steps to maintain the security and privacy of consumers' personally identifiable information (Minn. Stat. § 325M.05). Internet service providers are prohibited from knowingly disclosing personally identifiable information of their customers, subject to certain exceptions (Minn. Stat. § 325M.02). Exceptions permit disclosure upon subpoena, to law enforcement, by court order or warrant, to court in a civil action, to the customer by request, when incidental to the internet service provider's ordinary course of business, to other internet service providers for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the internet service provider or with the authorization of the consumer (Minn. Stat. § 325M.03; Minn. Stat. § 325M.04(1)).

Remedies: A consumer who prevails or substantially prevails in an action is entitled to recover the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded (Minn. Stat. § 325M.07).

3. Credit Card Data

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)).

Remedies: If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, that person or entity is required to reimburse the financial institution that issued any cards affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The financial institution may also recover costs for damages paid to cardholders injured by the breach (Minn. Stat. § 325E.64(3)).

4. Credit Reports

Security freeze: Consumers may request that a freeze be placed on their consumer reports either by certified mail, by telephone, or via a secure electronic mail connection provided by the consumer reporting agency (Minn. Stat. § 13C.016(2)). If a security freeze is placed on a consumer's credit report, consumer reporting agencies are prohibited from releasing information in the consumer's consumer report to a third party in connection with the extension of credit or the opening of an account without prior express authorization from the consumer (Minn. Stat. § 13C.016(1)(b)). A security freeze remains in place until the consumer requests that the security freeze be removed (Minn. Stat. § 13C.016(4)(e)).

> *Note: Federal legislation effective Sept. 21, 2018–the Economic Growth, Regulatory Relief, and Consumer Protection Act (Pub. L. No. 115-174)–establishes a national security freeze law applicable to consumers in general as well as to protected consumers (i.e., those under age 16 or those who are incapacitated or for whom a guardian or conservator has been appointed). The law amends provisions of the Fair Credit Reporting Act by establishing federal parameters for*

placing, temporarily lifting, or removing such freezes; it also prohibits the imposition of fees by a consumer reporting agency (CRA) for such services (15 U.S.C. § 1681c-1(i) and (j)). The federal law presumably preempts state law provisions governing security freezes. In the case of state fee provisions, the federal law is more favorable to consumers, but some states have stronger protections in their security freeze laws than those under the federal provision, including states that prohibit access to a security freeze for employer background checks. The federal law specifically permits access to a report subject to a freeze for such purposes.

Definitions: A consumer report is "a written, oral, or other communication of information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" that is used or expected to be used or collected in whole or in part for serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or certain authorized other purposes (Minn. Stat. § 13C.001(3)(a)).

Timing and procedure: A consumer reporting agency must place a security freeze on a consumer's consumer report no later than three business days after receiving a request from the consumer. Within ten business days after receiving the request, the consumer reporting agency is required to send a written confirmation of the security freeze to the consumer and provide the consumer with a unique PIN (personal identification number) or password to be used when providing authorization for the release of the consumer's consumer report for a specific party or period of time. When a consumer requests a security freeze, the consumer reporting agency must also disclose the process for placing and temporarily lifting a freeze (Minn. Stat. § 13C.016(3)).

Temporary lifting of security freeze: If the consumer wishes to allow his or her consumer report to be accessed for a specific party or period of time while a freeze is in place, the consumer must provide the consumer reporting agency with proper identification, a PIN or password previously provided by the agency, and proper information regarding the third party to receive the report. The consumer reporting agency must then process the request within three business days (Minn. Stat. § 13C.016(4)).

Permanent removal: If the consumer wishes to remove a security freeze, the consumer must provide the consumer reporting agency with proper identification and a PIN or password previously provided by the agency. The consumer reporting agency must then process the request within three business days (Minn. Stat. § 13C.016(4)(e)).

Fees: A consumer reporting agency may charge a fee of $5 for placing, temporarily lifting, or removing a security freeze. However, a customer who is the documented victim of identity theft may not be charged. If consumer fails to retain the original PIN given by the agency, the agency may charge an additional $5 dollar fee, except in cases of a one-time reissue of the same or a new PIN. Agencies may charge up to $5 for subsequent instances of loss of the PIN (Minn. Stat. § 13C.016(8)(a)-(b)).

Remedies: Any person or entity who violates the consumer security freeze provisions may be prosecuted by the attorney general and subject to an injunction or civil penalties not to exceed $25,000 (Minn. Stat. § 13C.04; Minn. Stat. § 8.31).

5. Criminal Records

Mandatory background checks: Every health-related licensing board must require all applicants to submit to both a state and national criminal history records check (Minn. Stat. § 214.075(1)(a)).

6. Drivers' Licenses/Motor Vehicle Records

Driver information services: Minnesota law requires the Commissioner of Public Safety to "establish written procedures to ensure that only individuals authorized by law may enter, update, or access not public data collected, created, or maintained by the driver and vehicle services information system," to revoke the authorization of anyone who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law, and to arrange an independent biennial audit of the information system to determine whether data are classified correctly, how data are used and for verifying compliance. This law also prohibits retention of certain data and requires the commissioner to notify applicants of retention procedures (Minn. Stat. § 171.12(3c)) and further prohibits the commissioner from electronically disseminating certain data outside the state, using certain out-of-state electronic validation verification systems, or sharing data with certain government agencies (Minn. Stat. § 171.12(7b); Minn. Stat. § 171.12(7c)).

Identify theft: Driver's license numbers are included in the definition of "Identity" that, if unlawfully obtained, is subject to Minnesota's identity theft law (Minn. Stat. § 609.527(1)(d)). For more information on identity theft, see Section I.G.2.

Breach notification: Driver's license numbers are included in the definition of "personal information" that, if unlawfully obtained, is subject to Minnesota's breach notification law (Minn. Stat. § 325E.61(1)(e)). For more information on breach notification, see Section I.C.8.

7. Electronic Communications/Social Media Accounts

Fiduciary access: Minnesota's Revised Uniform Fiduciary Access to Digital Assets Act allows custodian of deceased user to disclose the content of electronic communications sent or received by the user, along with certain other digital assets to a personal representative of the estate, upon consent from the user or direction of a court (Minn. Stat. § 521A.07 to Minn. Stat. § 521A.08).

Anti-spam: No person may send commercial electronic mail message that uses a third party's Internet domain name without permission of the third party, otherwise misrepresents any information in identifying the point of origin or transmission path of a commercial electronic mail message, or contains false or misleading information in the subject line (Minn. Stat. § 325F.694(2)). For more information on anti-spam provisions, see Section I.E.1.

8. Financial Information

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)).

Remedies: If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, that person or entity is required to reimburse the financial institution that issued any cards affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The financial institution may also recover costs for damages paid to cardholders injured by the breach (Minn. Stat. § 325E.64(3)).

Breach notification: Financial information, including account number, credit card or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, are included in the definition of "personal information" under Minnesota's breach notification law. For more information on breach notification, see Section I.C.8.

9. Health Data

Health records privacy: A health care service provider may not release a patient's health records to a person without a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release, specific authorization by law, or a representation from a provider that holds a signed and dated consent from the patient authorizing the release (Minn. Stat. § 144.293(2)). A health care service provider is a person that furnishes health care services, a licensed home care provider, a licensed health care facility, or a registered physician assistant (Minn. Stat. § 144.291(2)(i)).

Required notice of rights: A health care service provider must provide patients with a written notice concerning practices and rights with respect to access to health records. The notice must explain that disclosures of health records may be made without the written consent of the patient and that the patient maintains the right to access and obtain copies of the patient's health records and other information about the patient that is maintained by the provider (Minn. Stat. § 144.292(4)).

Exceptions: A health care service provider is not prohibited from disclosing the health records of a patient in the event of a medical emergency when the provider is unable to obtain the patient's consent or to other providers within related health care entities when necessary for the current treatment of the patient (Minn. Stat. § 144.293(5)).

A provider must disclose health records relating to a patient's mental health to a law enforcement agency if the agency provides the name of the patient and communicates that the patient is currently involved in an emergency interaction with the law enforcement agency that necessitates disclosure of the records to protect the health and safety of the patient or of another person (Minn. Stat. § 144.294(2)).

Access: Upon request, a health care service provider must provide complete and current information it possesses concerning the patient's diagnosis, treatment, and prognosis (Minn. Stat. § 144.292(2)). In addition, upon a patient's written request, a health care service provider must make available to the patient copies of the patient's health record at a reasonable cost (Minn. Stat. § 144.292(5)). With the consent of the patient, the health care service provider may instead furnish only a summary of the record. The health care service provider may exclude from the health record written speculations about the patient's health condition, except that all information necessary for the patient's informed consent must be provided (Minn. Stat. § 144.292(5)). However, if a health care service provider reasonably determines that the information is detrimental to the physical or mental health of the patient or is likely to cause the patient to inflict self-harm or to harm another, the health care service provider may withhold the information from the patient and may supply the information to an appropriate third party or to another provider (Minn. Stat. § 144.292(7)(a)).

Registries: Minnesota law prohibits any person or state that maintains or operates a registry of the names of persons, their human leukocyte antigen types and their willingness to be a tissue donor from revealing the identity of the person or the person's human leukocyte antigen type without the person's consent (Minn. Stat. § 144.336(1)).

Penalties: Any person who causes injury to a patient by releasing the health records of the patient either intentionally or negligently will be liable to the patient for compensatory damages, plus costs and reasonable attorney fees (Minn. Stat. § 144.298(2)).

Government-held data: Under the Minnesota Government Data Practices Act, health data on individuals created, collected, received, or maintained by the Department of Health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation necessary to analyze, describe, or protect the public health and medical data collected because an individual was or is a patient or client of a hospital, nursing home, medical center, clinic, health or nursing agency operated by a

government entity including business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual are considered private data and subject to the government data breach notification provisions (Minn. Stat. § 13.3805; Minn. Stat. § 13.384). For more information on government data collection laws, see Section I.C.2.

Insurance: Upon receiving a written request from an individual for access to personal information about the individual, an insurer, insurance agent, or insurance-support organization must inform the individual of the nature and substance of the personal information, including health information, that they possess; permit the individual to see and copy, in person, the personal information; permit the individual to obtain by mail a copy of all of the personal information or a reasonably described portion thereof; disclose to the individual the identity of those persons to whom the insurer, insurance agent, or insurance-support organization has disclosed the personal information within two years before the request; and provide the individual with a summary of the procedures by which the person may request correction, amendment, or deletion of personal information (Minn. Stat. § 72A.497(1); Minn. Stat. § 72A.497(3)).

10. Social Security Numbers

General data breach notification law: Social security numbers are included in the definition of "personal information" subject to the provisions of Minnesota's breach notification law (Minn. Stat. § 325E.61(1)(e)). For more information on the breach notification law, see Section I.C.8.

Social security number law: Regarding the use of social security numbers on or after July 1, 2008, a person or entity, not including a government entity, may not do any of the following:

- intentionally communicate or otherwise make available to the general public in any manner an individual's social security number;
- print an individual's social security number on any card required for the individual to access products or services provided by the person or entity;
- require an individual to transmit the individual's social security number over the Internet, unless the connection is secure or the social security number is encrypted, except as required by law;
- require an individual to use the individual's social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site;
- print a number that the person or entity knows to be an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed (if, in connection with a transaction involving or otherwise relating to an individual, a person or entity receives a number from a third party, that person or entity is under no duty to inquire or otherwise determine whether the number is or includes that individual's social security number and may print that number on materials mailed to the individual, unless the person or entity receiving the number has actual knowledge that the number is or includes the individual's social security number);
- assign or use a number as the primary account identifier that is identical to or incorporates an individual's complete social security number, except in conjunction with an employee or member retirement or benefit plan or human resource or payroll administration;
- sell social security numbers obtained from individuals in the course of business (not including the release of an individual's social security number if the release of the social security number is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose, but the release of a social security number for the purpose of marketing is not a legitimate business purpose); or

- restrict access to individual social security numbers it holds so that only its employees, agents, or contractors who require access to records containing the numbers in order to perform their job duties have access to the numbers, except as required by law.

However, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the social security number (but a social security number must not be included on the outside of a mailing or in the bulk mailing of a credit card solicitation offer).

The following are not prevented:

- the collection, use, or release of a social security number as required by state or federal law;
- the collection, use, or release of a social security number for a purpose specifically authorized or specifically allowed by a state or federal law that includes restrictions on the use and release of information on individuals that would apply to social security numbers; or
- the use of a social security number for internal verification or administrative purposes.

Documents that are recorded or required to be open to the public or by other law are excluded from the application of the foregoing (Minn. Stat. § 325E.59).

Identity theft: Social security numbers are included in the definition of "identity" that, if unlawfully obtained, is subject to Minnesota's identity theft law (Minn. Stat. § 609.527(1)(d)). For more information on identity theft, see Section I.G.2.

11. Usernames & Passwords

Data breach notification: Account numbers in combination with any required passwords that would permit access to an individual's financial account are included in the definition of "personal information" for purposes of Minnesota's breach notification law (Minn. Stat. § 325E.61(1)(e)).

12. Information about Minors

Government-held educational data: Any data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution that relates to a student may not be disclosed, except pursuant to court order, pursuant to specific authorization by statute and pursuant to certain other specified exceptions (Minn. Stat. § 13.32(3)).

Disclosure of educational data held by public institutions: Any data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution that relates to a student may not be disclosed, except pursuant to court order, pursuant to specific authorization by statute and pursuant to certain other specified exceptions (Minn. Stat. § 13.32(3)).

13. Location Data

Law enforcement activities: Upon receipt of a written request from a law enforcement agency, a wireless telecommunications service provider shall provide the requested call location information concerning a device to the requesting agency in order for the agency to respond to an emergency situation that involves the risk of death or serious physical harm to a person (Minn. Stat. § 237.83(1)).

Data protection for victims of violence: Actual or threatened victims of domestic violence, sexual assault, or stalking may enroll in a program to designate an alternate mailing address (Minn. Stat. § 5B.03). Once enrolled, address information collected by the secretary of state will be considered private data on individuals (Minn. Stat. § 5B.07). In addition, enrollees may request their landlords

to not display the enrollee's name at a protected address (Minn. Stat. § 5B.10). A violation may be punishable as a misdemeanor (Minn. Stat. § 5B.13).

14. Other Personal Data

Alcohol & drug test results: Test result reports and other information acquired in the drug or alcohol testing process are considered private and confidential information with respect to private sector employees and job applicants and private data on individuals with respect to public sector employees and job applicants. Such data may not be disclosed by an employer or laboratory to another employer or to a third-party individual, governmental agency, or private organization without the written consent of the employee or job applicant tested (Minn. Stat. § 181.954(2)).

E. SECTOR-SPECIFIC PROVISIONS

1. Advertising & Marketing

Anti-spam: No person may send commercial electronic mail message that uses a third party's Internet domain name without permission of the third party, otherwise misrepresents any information in identifying the point of origin or transmission path of a commercial electronic mail message, or contains false or misleading information in the subject line (Minn. Stat. § 325F.694(2)).

Mandatory subject disclosure: The subject line of a commercial electronic mail message must begin with "ADV", unless the message contains material of a sexual nature that may only be viewed by an individual at least 18 years of age, in which case the subject line must begin with "ADV-ADULT". This requirement does not apply if the recipient has consented to receive electronic mail messages from the sender, for organizations using electronic mail to communicate exclusively with their members, for entities that use electronic mail to communicate exclusively with their employees or contractors, or if there is a business or personal relationship between the sender and the recipient (Minn. Stat. § 325F.694(3)).

Opt-out: A sender initiating a commercial electronic mail message must establish a toll-free telephone number, a valid return electronic mail address, or another easy-to-use electronic method that the recipient may use to unsubscribe from any further messages (Minn. Stat. § 325F.694(4)).

Remedies: Any person injured by a violation of the anti-spam law may recover the lesser of $25 for each false or misleading message or $35,000 per day; or the lesser of $10 for each message sent not in compliance with the subject disclosure requirement or $25,000 per day. Attorney fees may also be awarded. In addition, violators may be prosecuted by the attorney general and subject to civil penalties not to exceed $25,000 (Minn. Stat. § 325F.694(7); Minn. Stat. § 8.31(3)).

Federal preemption: It should be noted that the federal CAN-SPAM Act preempts state laws that expressly regulate the use of electronic mail to send commercial messages, except to the extent that any such law prohibits falsity or deception in any portion of a commercial electronic mail message. Moreover, federal law does not preempt the applicability of state laws that are not specific to electronic mail, or other state laws to the extent that those laws relate to acts of fraud or computer crime.15 U.S.C. §7707(b).

Telemarketing: The use of automatic-dialing equipment is prohibited, unless the call is received between the hours of 9:00 a.m. and 9:00 p.m. (Minn. Stat. § 325E.30) and the subscriber has consented to receipt of the message or the message is immediately preceded by a live operator who obtains the subscriber's consent before the message is delivered (Minn. Stat. § 325E.27). This prohibition does not apply to messages (1) from school districts to students, parents, or employees; (2) to subscribers with whom the caller has a current business or personal relationship; (3) advising employees of work schedules; and (4) from a nonprofit tax-exempt charitable organization sent solely to solicit voluntary donations of clothing to benefit disabled military veterans and containing

no other solicitations (Minn. Stat. § 325E.27). Violators may be subject to investigation by the attorney general, civil penalties not to exceed $25,000, and liability for damages, including reasonable costs and fees, and other equitable relief (Minn. Stat. § 325E.31; Minn. Stat. § 8.31).

2. Education

Government-held data: Any data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution that relates to a student may not be disclosed, except pursuant to court order, pursuant to specific authorization by statute and pursuant to certain other specified exceptions (Minn. Stat. § 13.32). Government entities may only collect, store, use, or disseminate an individual's private or confidential data for the purposes given to the individual at the time of collection, unless an exception applies. Exceptions include cases where data collected before Aug. 1, 1975 and which have not been treated as public data, and which are used for purposes specifically approved by the Department of Administration, private or confidential data dissemination to individuals or entities specifically approved by the commissioner regarding the new purpose, upon consent of the data subject, or at certain meetings as permitted by law (Minn. Stat. § 13.05(4)). For more information on government data collection laws, see Section I.C.2.

Disclosure of educational data held by public institutions: Any data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution that relates to a student may not be disclosed, except pursuant to court order, pursuant to specific authorization by statute and pursuant to certain other specified exceptions (Minn. Stat. § 13.32(3)).

Student access to private records restricted: Students do not have the right of access to private data as to financial records and statements of the students' parents or any information therein (Minn. Stat. § 13.32(4)).

Cyberbullying: Minnesota's law to prevent student bullying encompasses "cyberbullying" and includes conduct that "violates a student's reasonable expectation of privacy" under Minnesota common law (Minn. Stat. § 121A.031(2)).

3. Electronic Commerce

Anti-spam: Minnesota law prohibits transmission of commercial electronic mail message that use a third party's Internet domain without permission, misrepresent their point of origin, contain false or misleading information in the subject line, or fail to contain information in the subject line designating the message as an advertisement (Minn. Stat. § 325F.694(2) to Minn. Stat. § 325F.694(3)). A sender initiating a commercial electronic mail message must establish a toll-free telephone number, a valid return electronic mail address, or another easy-to-use electronic method that the recipient may use to unsubscribe from any further messages (Minn. Stat. § 325F.694(4)). For more information on anti-spam laws, see Section I.E.1.

4. Financial Services

Electronic Funds Transfers: The person establishing and maintaining an electronic financial terminal, including any supporting equipment, structures or systems, must take such steps that are reasonably necessary to restrict disclosure of information to complete the transaction and to safeguard any information received or obtained about a customer or that customer's account from misuse by any person staffing an electronic financial terminal (Minn. Stat. § 47.69(1)).

Violations: Any customer of a financial institution may bring a civil action against any person in violation and, upon adverse adjudication, the defendant shall be liable for actual damages, or $500, whichever is greater, punitive damages when applicable, together with the court costs and reasonable attorneys' fees incurred by the plaintiff. The court also may provide equitable relief, including injunctive relief (Minn. Stat. § 47.69(5)).

5. Health Care

Notice of information practices: Minnesota law requires health care service providers to provide patients with a written notice concerning practices and rights with respect to access to health records. The notice must explain that disclosures of health records may be made without the written consent of the patient and that the patient maintains the right to access and obtain copies of the patient's health records and other information about the patient that is maintained by the provider (Minn. Stat. § 144.292(4)). Upon request, a health care service provider must provide complete and current information it possesses concerning the patient's diagnosis, treatment, and prognosis (Minn. Stat. § 144.292(2)). In addition, upon a patient's written request, a health care service provider must make available to the patient copies of the patient's health record at a reasonable cost (Minn. Stat. § 144.292(5)).

Access to health records: Upon receiving a written request from an individual for access to personal information about the individual, an insurer, insurance agent, or insurance-support organization must inform the individual of the nature and substance of the personal information, including health information, that they possess; permit the individual to see and copy, in person, the personal information; permit the individual to obtain by mail a copy of all of the personal information or a reasonably described portion thereof; disclose to the individual the identity of those persons to whom the insurer, insurance agent, or insurance-support organization has disclosed the personal information within two years before the request; and provide the individual with a summary of the procedures by which the person may request correction, amendment, or deletion of personal information (Minn. Stat. § 72A.497(1);(Minn. Stat. § 72A.497(3)).

6. HR & Employment

Drug & alcohol testing: Employers may require alcohol and drug testing of employees, or job applicants who have received a job offer, so long as the testing is performed pursuant to a written drug testing policy with certain specified content (Minn. Stat. § 181.951(1)). Labs may only disclose to employers test result data for alcohol and drugs present in samples tested (Minn. Stat. § 181.954). An employer or laboratory that violates sections of the drug and alcohol testing provisions is liable to an employee or job applicant injured by the violation in a civil action for any damages allowable at law. The court may also award reasonable attorney fees if the court finds that the employer acted knowingly or recklessly. Injured employees may also seek an injunction and reinstatement with back pay (Minn. Stat. § 181.956).

Genetic testing: Employers and employment agencies are prohibited from requesting or requiring protected genetic information regarding a person as a condition of employment. In addition, no person may provide employers with protected genetic information on any current or prospective employee (Minn. Stat. § 181.974(2)).

Payment for medical examinations: No employer may require an employee or applicant for employment to pay the cost of a medical examination or the cost of furnishing any medical records required by the employer as a condition of employment (Minn. Stat. § 181.61).

Mandatory background checks: Every health-related licensing board must require all applicants to submit to both a state and national criminal history records check (Minn. Stat. § 214.075(1)(a)).

Social media: Minnesota's Department of Employment and Economic Development published in 2013 "A Legal Guide to the Use of Social Media in the Workplace," which offers "a primer on the ways in which current law operates in areas like . . . ownership of social media accounts and content, privacy, and the relationship of a business' own use polices with the polices and terms of use of social media platforms."

7. Insurance

Access: Upon receiving a written request from an individual for access to personal information about the individual, an insurer, insurance agent, or insurance-support organization must inform the individual of the nature and substance of the personal information that they possess; permit the individual to see and copy, in person, the personal information; permit the individual to obtain by mail a copy of all of the personal information or a reasonably described portion thereof; disclose to the individual the identity of those persons to whom the insurer, insurance agent, or insurance-support organization has disclosed the personal information within two years before the request; and provide the individual with a summary of the procedures by which the person may request correction, amendment, or deletion of personal information (Minn. Stat. § 72A.497(1)).

Fees: An insurer, insurance agent, or insurance-support organization may charge an individual a reasonable fee, not to exceed the actual costs, to copy personal information, unless the individual is requesting information as a result of an adverse underwriting decision, in which case the insurer provide such information free of any charge (Minn. Stat. § 72A.497(4)).

Disclosure: An insurer, insurance agent, or insurance-support organization must not disclose any personal or privileged information about a person collected or received in connection with an insurance transaction without the authorization of that person, subject to certain exceptions (Minn. Stat. § 72A.502(1)).

Exceptions: There are numerous exceptions that permit insurers, insurance agents, or insurance-support organizations to disclose personal or privileged information without an individual's consent. These include for purposes of detecting fraud or criminal activity; as is reasonably necessary during a merger or sale; or for research purposes, among others (Minn. Stat. § 72A.502(1) to Minn. Stat. § 72A.502(11a)).

Remedies: Insurers, insurance agents, or insurance-support organizations who violate the personal information privacy provisions of the Minnesota Insurance Fair Information Reporting Act are liable to the injured parties for any damages sustained, plus costs and reasonable attorney fees. Equitable and declaratory relief may also be granted. In the case of a willful violation, the injured party will also be entitled to exemplary damages of not less than $1,000 nor more than $15,000 for each violation (Minn. Stat. § 72A.503; Minn. Stat. § 13.08(1)).

8. Retail & Consumer Products

Credit card data retention: Any person or entity conducting business in Minnesota who accepts credit cards, debit cards, stored value cards, and other forms of "access devices" is prohibited from retaining any "card security code data, PIN verification code number, or the full contents of any track of magnetic stripe data," after the authorization of the transaction or, for debit cards, for more than 48 hours after the authorization of the transaction (Minn. Stat. § 325E.64(2)).

Remedies: If a breach of the security of the system occurs involving data held by a person or entity doing business in Minnesota in violation of these data retention provisions, that person or entity is required to reimburse the financial institution that issued any cards affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The financial institution may also recover costs for damages paid to cardholders injured by the breach (Minn. Stat. § 325E.64(3)).

9. Social Media

Minnesota's law to prevent student bullying encompasses "cyberbullying" and includes conduct that "violates a student's reasonable expectation of privacy" under Minnesota common law (Minn. Stat. § 121A.031(2).

Minnesota's Department of Employment and Economic Development published in 2013 "A Legal Guide to the Use of Social Media in the Workplace," which offers "a primer on the ways in which current law operates in areas like . . . ownership of social media accounts and content, privacy, and the relationship of a business' own use polices with the polices and terms of use of social media platforms."

10. Tech & Telecom

Anti-spam: No person may send commercial electronic mail message that uses a third party's Internet domain name without permission of the third party, otherwise misrepresents any information in identifying the point of origin or transmission path of a commercial electronic mail message, or contains false or misleading information in the subject line (Minn. Stat. § 325F.694(2)). For more information on anti-spam laws, see Section I.E.1.

Internet service providers: Internet service providers must take reasonable steps to maintain the security and privacy of consumers' personally identifiable information (Minn. Stat. § 325M.05). Internet service providers are prohibited from knowingly disclosing personally identifiable information of their customers, subject to certain exceptions (Minn. Stat. § 325M.02). Exceptions permit disclosure upon subpoena, to law enforcement, by court order or warrant, to court in a civil action, to the customer by request, when incidental to the internet service provider's ordinary course of business, to other internet service providers for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the internet service provider or with the authorization of the consumer (Minn. Stat. § 325M.03; Minn. Stat. § 325M.04(1)).

Remedies: A consumer who prevails or substantially prevails in an action is entitled to recover the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded (Minn. Stat. § 325M.07).

11. Other Sectors

Government Data:

In general: Government entities may only collect, store, use, or disseminate an individual's private or confidential data for the purposes given to the individual at the time of collection, unless an exception applies. Exceptions include cases where data collected before Aug. 1, 1975 and which have not been treated as public data, and which are used for purposes specifically approved by the Department of Administration, private or confidential data dissemination to individuals or entities specifically approved by the commissioner regarding the new purpose, upon consent of the data subject, or at certain meetings as permitted by law (Minn. Stat. § 13.05(4)). The state official designated as the responsible authority must establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that is not public is only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure as well as establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected, and develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law (Minn. Stat. § 13.05(5)(a)). At least once a year, each government entity is required to conduct a comprehensive security assessment of any personal information it maintains (Minn. Stat. § 13.055(6)). When disposing of not public data, the data must be destroyed in a way that prevents its contents from being determined (Minn. Stat. § 13.05(5)(b)).

Driver information services: Minnesota law requires the Commissioner of Public Safety to "establish written procedures to ensure that only individuals authorized by law may enter, update, or access not public data collected, created, or maintained by the driver and vehicle services information

system," to revoke the authorization of anyone who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law, and to arrange an independent biennial audit of the information system to determine whether data are classified correctly, how data are used and for verifying compliance. This law also prohibits retention of certain data and requires the commissioner to notify applicants of retention procedures (Minn. Stat. § 171.12(3c)) and further prohibits the commissioner from electronically disseminating certain data outside the state, using certain out-of-state electronic validation verification systems, or sharing data with certain government agencies (Minn. Stat. § 171.12(7b); Minn. Stat. § 171.12(7c)).

Breach notification: A government entity that collects, creates, receives, maintains, or disseminates private or confidential information on individuals must disclose any breach of the security to any individual whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay (Minn. Stat. § 13.055(2)(a)).

F. Electronic Surveillance

Subject to certain exceptions, the intentional interception of any type of wire, electronic, or oral communication constitutes a criminal violation under the Minnesota criminal code. In addition, subject to certain exceptions, the intentional disclosure to any other person or use of the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication, is also prohibited. Such violations are subject to a fine of not more than $20,000, imprisonment of not more than 5 years, or both (Minn. Stat. § 626A.02(1); Minn. Stat. § 626A.02(4)).

Exceptions: Minnesota law does not prohibit interception of a communication if done by a person not acting under color of law is a party to the communication or if one of the parties to the communication has given prior consent to such interception, so long as the communication is not intercepted for the purpose of committing any criminal or tortious act (Minn. Stat. § 626A.02(2)(d)).

It is not unlawful for switchboard operator or a provider of wire or electronic communication service to intercept, disclose, or use a communication in the normal course of employment and for a purpose that is a necessary incident to the provision of service or to the protection of the service provider's rights or property, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks (Minn. Stat. § 626A.02(2)(a)).

Additional specific exemptions apply, including interceptions of communications by the Federal Communications Commission; communications open to the general public; communications transmitted by government or law enforcement communication systems; communications made within bands designated for amateur, citizens band, or mobile radio services; or communications that are causing harmful interference to equipment, among others (Minn. Stat. § 626A.02(2)).

A civil action is available for persons whose wire, electronic, or oral communications have been unlawfully intercepted. A court may assess as damages the greater of the sum of three times the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, or statutory damages equal to the greater of $100 for each day of violation or $10,000 (Minn. Stat. § 626A.13(3)(b)).

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Electronic Funds Transfers: Any customer of a financial institution may bring a civil action against any person in violation and, upon adverse adjudication, the defendant shall be liable for actual damages, or $500, whichever is greater, punitive damages when applicable, together with the court costs and reasonable attorneys' fees incurred by the plaintiff. The court also may provide equitable relief, including injunctive relief (Minn. Stat. § 47.69(5)).

Security freeze: Any person injured by a violation of the consumer security freeze laws may bring a civil action and recover damages, together with costs and disbursements, including costs of investigation and reasonable attorney fees, and receive other equitable relief as determined by the court (Minn. Stat. § 13C.04; Minn. Stat. § 8.31(3a)).

Telemarketing: Violators may be subject to investigation by the attorney general, civil penalties not to exceed $25,000, and liability for damages, including reasonable costs and fees, and other equitable relief (Minn. Stat. § 325E.31; Minn. Stat. § 8.31).

Video services: Any person injured by actions of a video seller or service in violation of consumer data privacy provisions who prevails in a civil action is entitled to a minimum of $500 damages, regardless of the amount of actual damage proved, together with costs, disbursements, and reasonable attorney fees, in addition to being subject to prosecution by the attorney general (Minn. Stat. § 325I.03; Minn. Stat. § 8.31(2)).

Internet service providers: Consumers injured by an internet service provider's failure to take reasonable steps to maintain the security and privacy of a consumer's personally identifiable information may sue to recover the greater of $500 or actual damages. Costs, disbursements, and reasonable attorney fees may be awarded (Minn. Stat. § 325M.05; Minn. Stat. § 325M.07).

2. Identity Theft

In general: Minnesota law makes it a crime to transfer, possess, or use another person's identity with the intent to commit, aid, or abet unlawful activity (Minn. Stat. § 609.527). A person convicted of committing identity theft may be ordered to pay restitution of at least $1,000 to each direct victim (Minn. Stat. § 609.527(4)(b)).

3. Invasion of Privacy

Health data: Any person who causes injury to a patient by releasing the health records of the patient either intentionally or negligently will be liable to the patient for compensatory damages, plus costs and reasonable attorney fees (Minn. Stat. § 144.298(3)).

Insurance: Insurers, insurance agents, or insurance-support organizations who violate the personal information privacy provisions of the Minnesota Insurance Fair Information Reporting Act are liable to the injured parties for any damages sustained, plus costs and reasonable attorney fees. Equitable and declaratory relief may also be granted. In the case of a willful violation, the injured party will also be entitled to exemplary damages of not less than $1,000 nor more than $15,000 for each violation (Minn. Stat. § 72A.503; Minn. Stat. § 13.08(1)).

4. Other Causes of Action

Anti-spam: Any person injured by a violation of the anti-spam law may recover the lesser of $25 for each false or misleading message or $35,000 per day; or the lesser of $10 for each message sent not in compliance with the subject disclosure requirement or $25,000 per day. Attorney fees may also be awarded. For more information on anti-spam laws, see Section I.E.1.

Electronic surveillance: A person whose wire, oral, or electronic communication is unlawfully intercepted may recover from the person or entity that engaged in that violation relief as may be appropriate in a civil action. Appropriate relief includes temporary and other equitable or declaratory relief as may be appropriate, damages and punitive damages in appropriate cases, and reasonable attorney's fees and other litigation costs reasonably incurred (Minn. Stat. § 626A.13(2)). The court may assess as damages the greater of the sum of three times the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, or statutory damages equal to the greater of $100 a day for each day of violation or $10,000 (Minn. Stat. § 626A.13(3)(b)).

H. CRIMINAL LIABILITY

Video services: Video sellers or services who violate consumer data protection provisions may be subject to prosecution by the attorney general (Minn. Stat. § 325I.03; Minn. Stat. § 8.31(2)). For more information on consumer data privacy laws, see Section I.D.2.

Data breach: Violators of the data breach notification requirements may be prosecuted by the attorney general (Minn. Stat. § 325E.61(6); Minn. Stat. § 8.31(2)). For more information on breach notification provisions, see Section I.C.8.

Data protection for victims of violence: Actual or threatened victims of domestic violence, sexual assault, or stalking may enroll in a program to designate an alternate mailing address (Minn. Stat. § 5B.03). Once enrolled, address information collected by the secretary of state will be considered private data on individuals (Minn. Stat. § 5B.07). In addition, enrollees may request their landlords to not display the enrollee's name at a protected address (Minn. Stat. § 5B.10). A violation may be punishable as a misdemeanor (Minn. Stat. § 5B.13). For more information, see Section I.D.13.

Electronic surveillance: Minnesota imposes criminal penalties for various types of invasion of privacy. Subject to certain exceptions, anyone who intentionally intercepts, discloses, or uses any wire, electronic, or oral communication is subject to a fine of not more than $20,000, imprisonment of not more than 5 years, or both (Minn. Stat. § 626A.02(1); Minn. Stat, § 626A.02(4)). For more information on electronic surveillance, see Section I.F.

Security freeze: Violators of the consumer security freeze requirements may be prosecuted by the attorney general (Minn. Stat. § 13C.04; Minn. Stat. § 8.31(3)). For more information on consumer security freezes, see Section I.D.4.

Telemarketing: Violators of the restrictions on the use of automatic-dialing equipment may be subject to prosecution by the attorney general (Minn. Stat. § 325E.31; Minn. Stat. § 8.31(2)). For more information on telemarketing regulations, see Section I.E.1.

Identity theft: Minnesota law makes it a crime to transfer, possess, or use another person's identity with the intent to commit, aid, or abet unlawful activity (Minn. Stat. § 609.527(2)). Violators are subject to penalties of imprisonment up to 20 years, a fine of up to $100,000, or both (Minn. Stat. § 609.527(3); Minn. Stat. § 609.52(3)).

Revenge porn: Minnesota law makes it a gross misdemeanor to intentionally disseminate the image of another identifiable person depicted in a sexual act or whose intimate parts are exposed when the actor knows or reasonably should have known the person depicted had a reasonable expectation of privacy and does not consent to dissemination (Minn. Stat. § 617.261(1). Violators are subject to a fine of $5,000, imprisonment of up to three years, or both (Minn. Stat. § 617.261(2)).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. ATTORNEY GENERAL

The attorney general is responsible for enforcing a number of Minnesota's privacy provisions (see Minn. Stat. § 8.31), including:

- private data breach notification law (Minn. Stat. § 325E.61(6));
- restrictions on the use of automatic dialing equipment (Minn. Stat. § 325E.31);
- the Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68 to Minn. Stat. § 325F.70);
- security freeze requirements (Minn. Stat. § 13C.04); and
- video services provisions (Minn. Stat. § 325I.03).

B. OTHER REGULATORS

The Department of Health administers the Medical Records Act (Minn. Stat. § 144.291 to Minn. Stat. § 144.34), which establishes rules to protect the confidentiality of patient records by health care providers.

The Commissioner of Commerce is responsible for enforcing the Minnesota Insurance Fair Information Reporting Act, which includes provisions regarding patient right-of-access to information held by insurers, insurance agents, or insurance-support organizations (Minn. Stat. § 72A.497; Minn. Stat. § 60A.03(2)).

C. SANCTIONS & FINES

Anti-spam: Any person injured by a violation of the anti-spam law may recover the lesser of $25 for each false or misleading message or $35,000 per day; or the lesser of $10 for each message sent not in compliance with the subject disclosure requirement or $25,000 per day. Attorney fees may also be awarded. In addition, violators may be prosecuted by the attorney general and subject to civil penalties not to exceed $25,000 (Minn. Stat. § 325F.694(7); Minn. Stat. § 8.31(3)). For more information on anti-spam laws, see Section I.E.1.

Video services: Video sellers or services who violate consumer data privacy provisions may be subject to civil penalties not to exceed $25,000 (Minn. Stat. § 325I.03; Minn. Stat. § 8.31(2)). For more information on consumer data privacy laws, see Section I.D.2.

Security freeze: Violators of the consumer security freeze requirements may be subject to civil penalties not to exceed $25,000 (Minn. Stat. § 13C.04; Minn. Stat. § 8.31(4)). For more information on consumer security freezes, see Section I.D.4.

Telemarketing: Violators of the restrictions on the use of automatic-dialing equipment may be subject to civil penalties not to exceed $25,000 (Minn. Stat. § 325E.31; Minn. Stat. § 8.31(2)). For more information on telemarketing regulations, see Section I.E.1.

Breach notification: The attorney general may seek fines up to $25,000 for violations of Minnesota's breach notification requirements (Minn. Stat. § 325E.61(6); Minn. Stat. § 8.31(3)). For more information on breach notification provisions, see Section I.C.8.

Electronic surveillance: Subject to certain exceptions, anyone who intentionally intercepts, discloses, or uses any wire, electronic, or oral communication is subject to a fine of not more than $20,000, imprisonment of not more than 5 years, or both (Minn. Stat. § 626A.02(1); Minn. Stat, § 626A.02(4)). For more information on electronic surveillance, see Section I.F.

D. REPRESENTATIVE ENFORCEMENT ACTIONS

1. Sellers Playbook

In November 2018, the Minnesota Attorney General and the Federal Trade Commission entered into a settlement with Sellers Playbook/Exposure Marketing and Matthew and Jessie Tieva regarding charges of running a large business opportunity scheme. The settlement imposed a $20.8 million judgment against the defendants, which will be suspended when they surrender all funds held in any corporate accounts, all goods and assets owned by the corporate defendants, all assets held by the court-appointed receiver, and substantial assets owned by Matthew and Jessie Tieva. The settlement also prohibits the defendants from selling or assisting others to sell any business opportunity or business coaching program and from making unsupported earnings claims and suppressing consumers' reviews of defendants' products or services, and requires that significant assets be turned over for consumer redress.

2. Target

In May 2017, the Minnesota Attorney General entered into an assurance of voluntary compliance with Target to settle a multi-state investigation in response to the security incident announced by Target in late 2013. Target agreed to pay $18.5 million to the Attorneys General, of which Minnesota received $283,736.

3. Adobe Systems

On Nov. 10, 2016, Minnesota joined 15 other states in a $1 million no-fault settlement with the software company Adobe Systems Inc. to end enforcement actions that charged the company didn't have proper measures in place to protect its systems from cyberattack.

4. Accretive Health

The Commissioner of the Minnesota Department of Commerce entered into a Consent Cease and Desist Order with Accretive Health in February 2012 whereby Accretive voluntarily agreed to cease all debt collection activity in Minnesota. In July 2012, the Minnesota Attorney General and Accretive entered into a settlement agreement, release and order (the "Settlement Agreement ") to settle the Minnesota Attorney General's lawsuit against Accretive. The Settlement Agreement included a $2,490,400 settlement sum.

E. STATE RESOURCES

The Minnesota Attorney General has information on its website for consumers regarding unwanted calls, scams, and identity theft, among numerous others.

III. RISK ENVIRONMENT

The Minnesota Attorney General, the Minnesota Department of Commerce, and the Federal Trade Commission have taken actions against companies and individuals, and the Minnesota Office of the Legislative Auditor has conducted special reviews and issued reports regarding state government. Following are summaries, including the laws involved.

Actions against companies and individuals relate to Medical Informatics Engineering d/b/a Enterprise Health and K&L Holdings/NoMoreClipboard, Sellers Playbook/Exposure Marketing and Matthew and Jessie Tieva, Target Corporation, Adobe Systems, and Accretive Health, Inc.

In December 2018, Minnesota and 11 other states charged Medical Informatics Engineering d/b/a Enterprise Health and K&L Holdings/NoMoreClipboard with violations of the Minnesota Deceptive

Trade Practices Act (Minn. Stat. § 325D.43 et seq.), the Minnesota Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68 et seq.), the Minnesota general data breach notification law (Minn. Stat. § 325E.61), the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 1302(a)), and the Department of Health and Human Services Regulations (45 C.F.R. § 160 et seq.), relating to a security incident from June 2015. The complaint is notable because it marks the first time state attorneys general have sued in federal court under HIPAA for a data breach incident. *Indiana v. Medical Informatics Engineering Inc.*, No. 18-cv-00969 (N.D. Ind., filed Dec. 4, 2018).

In November 2018, the Minnesota Attorney General and the Federal Trade Commission entered into a settlement with Sellers Playbook/Exposure Marketing and Matthew and Jessie Tieva regarding charges of running a large business opportunity scheme in violation of the Minnesota Deceptive Trade Practices Act (Minn. Stat. § 325D.43 et seq.), the Minnesota Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68 et seq.), the Federal Trade Commission Act (15 U.S.C. §45(a)), the Business Opportunity Rule (16 C.F.R. § 437.01 et seq.), and the Consumer Review Fairness Act of 2016 (15 U.S.C. § 45b). The settlement imposed a $20.8 million judgment against the defendants, which will be suspended when they surrender all funds held in any corporate accounts, all goods and assets owned by the corporate defendants, all assets held by the court-appointed receiver, and substantial assets owned by Matthew and Jessie Tieva. The settlement also prohibits the defendants from selling or assisting others to sell any business opportunity or business coaching program and from making unsupported earnings claims and suppressing consumers' reviews of defendants' products or services, and requires that significant assets be turned over for consumer redress.

In May 2017, the Minnesota Attorney General entered into an assurance of voluntary compliance with Target to settle a multi-state investigation in response to the security incident announced by Target in late 2013. Target agreed to pay $18.5 million to the Attorneys General, of which Minnesota received $283,736. Under the settlement, Target was required to adopt certain measures to secure customers' information. The settlement required Target to comply with the Minnesota Deceptive Trade Practices Act (Minn. Stat. § 325D.43 to Minn. Stat. § 325D.48), the Minnesota Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68 to Minn. Stat. § 325F.70), the Minnesota social security number law (Minn. Stat. § 325E.59), the Minnesota credit card data law (Minn. Stat. § 325E.64), and the Minnesota general data breach notification law (Minn. Stat. § 325E.61), to implement and maintain a comprehensive information security program (including employing an executive to oversee such program and to advise its CEO and board), to encrypt or otherwise protect payment card information, and to adopt certain other measures.

In November 2016, Minnesota joined 15 other states in a $1 million no-fault settlement with the software company Adobe Systems to end enforcement actions alleging the company didn't have proper measures in place to protect its systems from cyberattack.

In connection with the theft in Minnesota in July 2011 of an Accretive employee's laptop that contained protected health information, the Commissioner of the Minnesota Department of Commerce entered into a Consent Cease and Desist Order with Accretive in February 2012 whereby Accretive voluntarily agreed to cease all debt collection activity in Minnesota. In July 2012, the Minnesota Attorney General and Accretive entered into a settlement agreement, release and order (the "Settlement Agreement") to settle the Minnesota Attorney General's lawsuit against Accretive in which violations of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17930), the Minnesota Health Records Act (Minn. Stat. § 144.291 et seq.), the Minnesota Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68 to Minn. Stat. § 325F.70), and certain Minnesota consumer protection and debt collection laws were alleged in connection with such laptop theft, and all investigations relating to Accretive by the Minnesota Attorney General, the

Minnesota Department of Commerce and the Minnesota Department of Human Services. The Settlement Agreement included a $2,490,400 settlement sum, Accretive's voluntary agreement to wind down Accretive's Minnesota business operations, to destroy or return to any Minnesota client all protected health information and personal financial information in its possession, and to not conduct business in Minnesota, or on behalf of a Minnesota client, for a two-year period following the wind down date (other than any continuation of prior licensing of Accretive's technology), and the contemplation of potential restrictions on any future Minnesota operations should Accretive choose to resume operations in Minnesota in accordance with the terms of the Settlement Agreement.

For information about the Minnesota Attorney General regarding emerging issues and outlook, see Section IV.C.

Minn. Stat. § 3.971(6a) authorizes the Minnesota Office of the Legislative Auditor (OLA) to conduct data security audits on state agencies, departments, boards, commissions, offices, courts, and other organizations subject to audit by the legislative auditor. In 2013, OLA conducted a review of MNsure (the state agency that manages Minnesota's health insurance exchange) after an unauthorized disclosure by a MNsure employee of private data (including social security numbers). OLA issued a 2013 report concluding, among other things, that MNsure officials made decisions that contributed directly to the unauthorized disclosure.

OLA also conducted a review of the state government's use of a private vendor, Lookout Services, Inc., to help implement E-Verify. In late 2009, Minnesota suspended its agreement with Lookout after state officials received a second notice that not public data on its website could be accessed without adequate security protection. OLA issued a 2010 report in which it recommended that state government conduct and document an assessment of the security risks and how those risks will be addressed when seeking services from an information technology vendor that involve the vendor obtaining, processing, transmitting, or storing not public data and ensure that information security specialists are fully involved in the process of identifying, selecting, contracting with, and monitoring the performance of the vendor. OLA also recommended that state government establish policies and procedures for state agencies to follow regarding the use of information technology vendors.

IV. EMERGING ISSUES AND OUTLOOK

A. RECENT LEGISLATION

1. Interference with Electronic Terminals

Legislation, approved by the Governor on May 8, 2018, establishes crimes for interfering or attempting to interfere with an "electronic terminal," defined as "an electronic device . . . through which an individual or company may initiate an electronic fund transfer. The term includes, but is not limited to, point-of-sale terminals, automated teller machines, cash dispensing machines, and gas pump dispensers." Among other things, the legislation amends Minnesota's computer crime provisions by specifying that a person "is guilty of unauthorized computer access if the person intentionally and without authorization attempts to or does penetrate a computer security system *or electronic terminal*." Minn. Stat. § 609.891 (emphasis added). 2018 Minn. Sess. Laws ch. 123. Effective Aug. 1, 2018.

2. Driver's Licenses

Minnesota's Real ID Act (2017 Minn. Laws Ch. 76), passed in May 2017 and effective in July 2017, requires the Commissioner of Public Safety to "establish written procedures to ensure that only

individuals authorized by law may enter, update, or access not public data collected, created, or maintained by the driver and vehicle services information system," to revoke the authorization of anyone who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law, and to arrange an independent biennial audit of the information system to determine whether data are classified correctly, how data are used and for verifying compliance (Minn. Stat. § 171.12(1a)). This law also prohibits retention of certain data and requires the commissioner to notify applicants of retention procedures (Minn. Stat. § 171.12(3c)) and further prohibits the commissioner from electronically disseminating certain data outside the state, using certain out-of-state electronic validation verification systems, or sharing data with certain government agencies (Minn. Stat. § 171.12(7b); Minn. Stat. § 171.12(7c)).

B. PROPOSED LEGISLATION (90TH LEGISLATURE, 2017-2018)

1. Social Media

HF 4472, introduced May 1, 2018, would create a social media bill of rights, governing disclosure of personal information, and create a cause of action and civil penalty for violations of such bill of rights.

2. Data Sharing

HF 4457, introduced Apr. 23, 2018, would establish the Vulnerable Adult Maltreatment Prevention and Accountability Act and modify, among other things, requirements for data sharing and data classifications. A similar bill, HF 4458, was also introduced Apr. 23, 2018.

3. Background Checks

SF 3953, introduced Apr. 12, 2018, would, among other things, require criminal history background checks for teachers and other school employees.

4. Credit Reports and Security Freezes

SF 3881, introduced Mar. 29, 2018, prohibits a consumer reporting agency from charging a fee related to placing or lifting a security freeze when the consumer reporting agency notifies a customer of a data breach involving information in a consumer report. A companion measure, HF 4277, was introduced Mar. 28, 2018.

5. Internet Privacy

SF 2438, introduced May 22, 2017, and HF 4182, introduced Mar. 22, 2018, would require telecommunications service providers to comply with Internet privacy requirements.

In April 2017, the Minnesota House and Senate initially passed a bill that would require Internet service providers to secure user consent before collecting private data. However, the bill was revised, and the language pertaining to Internet privacy was removed.

HF 2606 (SF 2323) and HF 2579 (SF 2309), both also introduced in April 2017, address internet service providers and internet privacy requirements.

6. Smartphone Monitoring

HF 2651, introduced May 8, 2017, would prohibit a private entity from activating or enabling the microphone of a digital device owned by a consumer in order to listen, store, transmit, or disclose the information accessed unless certain conditions are satisfied.

7. Social Media Privacy

HF 2591 (SF 2320), introduced Apr. 7, 2017, would prohibit employers and educational institutions from requiring, coercing, or requesting students or employees to provide access information

relating to, online accounts protected by log-in information. The law would allow the attorney general or a student or employee to bring a civil action for violations.

HF 2116 (SF 2038), introduced Mar. 6, 2017, would prohibit employers from requiring, coercing, or requesting employees to provide access information relating to personal social media accounts.

8. Education

HF 2118, introduced Mar. 6, 2017, would prohibit educational institutions from accessing or compelling a student to produce, display, share, or provide access to data stored upon or accessible from a student's personal technological device, subject to certain conditions, and would allow an injured party to seek damages or equitable relief for a violation.

HF 1507 (SF 1961) introduced Feb. 20, 2017, would amend the Minnesota Government Data Practices Act regarding educational data.

HF 307, introduced Jan. 17, 2017, would enact the Student Online Data Protection and Privacy Act relating to educational data, protecting online student data and establishing student digital privacy rights.

C. OTHER ISSUES

1. Equifax Breach

In September 2017, Minnesota Attorney General Lori Swanson joined other attorneys general in an investigation into the Equifax data breach. In a letter sent to Equifax Sept. 15, the attorneys general called for Equifax to disable links for enrollment in fee-based credit monitoring service in the wake of the massive data breach.

2. Proposed Federal Legislation

In March 2018, Minnesota Attorney General Lori Swanson joined other attorneys general in a letter sent to U.S. House of Representatives committee leaders regarding the proposed Data Acquisition and Technology Accountability and Security Act, stating that Congress should not preempt state data security and breach notification laws.

3. Facebook/Cambridge Analytica

In March 2018, Minnesota Attorney General Lori Swanson joined other attorneys general in a letter sent to Facebook CEO Mark Zuckerberg, asking questions about data-sharing procedures that led to the alleged use of 50 million users' data without their consent by Cambridge Analytica. The National Association of Attorneys General seeks information about how the company will make privacy policies and terms of service clearer and more understandable; what controls the company has over data given to developers; what safeguards are in place to police these activities; and what kinds of user data the social media giant knew Cambridge Analytica was accessing and using, and when.

Facebook sent a detailed response to the National Association of Attorneys General on May 7, 2018, that outlines the company's policies and practices regarding user data, the facts related to the misuse of data, and the steps Facebook is taking to address the incident and prevent any recurrence.

4. HIPAA Enforcement Action

On Dec. 4, 2018, the Minnesota Attorney General joined attorneys general from 11 other states in suing two medical IT companies for poor security practices that allegedly led to theft of medical information from nearly 4 million patients. The complaint marks the first time state attorneys general have sued in federal court under the Health Insurance Portability and Accountability Act

(HIPAA) for a data breach incident. The complaint alleges that Fort Wayne, Ind.-based companies Medical Informatics Engineering, Inc. and NoMoreClipboard, LLC failed to take "reasonable measures" to protect their computer systems and failed to provide timely and adequate notice of a breach that occurred in 2015. The attorneys general brought the action pursuant to 42 U.S.C. § 1320d-5(d) –which authorizes attorneys general to initiate federal district court proceedings for HIPAA violations. The complaint also includes state law claims, alleging violations of unfair and deceptive practice laws, breach notification statutes, and personal information protection acts. *Indiana v. Medical Informatics Engineering, Inc.*, No. 1:18-cv-00969 (N.D. Ind., filed Dec. 4, 2018).

