Bloomberg Law

Privacy Profile

State Profile, Idaho

Claire C. Rosston and Tracy Gray,
Holland & Hart LLP

State Profile, Idaho

Claire C. Rosston and Tracy Gray, of Holland & Hart LLP, provided expert review of the Idaho Profile and wrote the Risk Environment section.

I. APPLICABLE LAWS AND REGULATIONS

A. Constitutional Provisions –

There are no constitutional provisions in Idaho conferring a general right of privacy on Idaho residents.

B. Personal Data Protection Provisions –

The primary privacy and data security law in Idaho is the state's data breach notification law (Idaho Code § 28-51-104 through Idaho Code § 28-51-107), which is outlined below and discussed in detail at Section I.C.8.

There are additional privacy laws in Idaho, including laws governing security freezes (see Section I.D.4.), electronic surveillance (see Section I.F.), and identity theft (see Section I.G.2.). Finally, laws related to privacy and data security applicable to specific sectors, such as health care, insurance, and employment, are set forth in the portions of this profile dedicated to those sectors.

1. Who is covered? –

The data breach notification law applies to any resident of Idaho whose personal information was or is reasonably believed to have been misused (Idaho Code § 28-51-105(1)).

2. What is covered? –

The data breach notification law requires a city, county, or state agency, an individual, or a commercial entity conducting business in Idaho and owning or licensing computerized data that includes personal information about Idaho residents to conduct an investigation, upon becoming aware of a breach of the security of the system, to determine the likelihood that personal information has been or will be misused, and on finding such misuse or potential misuse, to notify affected Idaho residents (Idaho Code § 28-51-105(1)). In addition, an agency, individual, or commercial entity that maintains computerized data containing personal information that it does not own or license must give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information of an Idaho resident has occurred or is likely to occur (Idaho Code § 28-51-105(2)). For specific information on breach notification requirements, see Section I.C.8.

3. Who must comply? –

The data breach notification law applies to all city, county, or state agencies, individuals, and commercial entities that conduct business in Idaho and own or license computerized data that includes personal information about an Idaho resident (Idaho Code § 28-51-105(1)). A "commercial entity" includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, or any other legal entity, whether for profit or not for profit (Idaho Code § 28-51-104(3)).

C. Data Management Provisions

1. Notice & Consent –

Data breach notification: For information on notice requirements under the state's data breach notification requirements, see Section I.C.8.

Electronic surveillance: For information on consent requirements regarding the recording of telephone conversations in Idaho, see Section I.F.

2. Collection & Use –

Insurance and health provisions: Idaho insurance laws and regulations governing the privacy of nonpublic personal information of consumers contain provisions regarding collection and use of such information (see **Section I.E.7.**). In addition, provisions of Idaho law governing specific types of health care facilities and providers and health data contain requirements regarding collection and use of such data (see Section I.D.9.).

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), the Department of Education is required to develop policies for school districts and public charter schools governing data collection and use (see Section I.E.2.).

3. Disclosure to Third Parties –

Insurance and health provisions: Idaho insurance laws and regulations governing the privacy of nonpublic personal information of consumers contain provisions regarding the disclosure of such information (see Section I.E.7.). In addition, provisions of Idaho law governing specific types of health care facilities and providers and health data contain requirements regarding disclosure of such data (see Section I.D.9.). Finally, laws governing children's mental health services contain specific requirements regarding disclosure of treatment information to parents or others (see Section I.D.12.).

Records not subject to disclosure under Public Records Act: A variety of specified records are not subject to disclosure under the Idaho Public Records Act, including records exempt from disclosure under state or federal law or federal regulations, or records contained in court files not subject to disclosure under the rules of the Idaho Supreme Court (Idaho Code § 74-104); law enforcement and investigatory records, evacuation and emergency response plans, and worker's compensation records (Idaho Code § 74-105); and various personnel records, health records, and other records containing personal information (Idaho Code § 74-106). For a comprehensive discussion of the Public Records Act, see Section I.C.10.

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), certain disclosures of student data are prohibited, and the Department of Education is required to develop policies for school districts and public charter schools governing disclosures (see Section I.E.2.).

4. Data Storage –

Our research has revealed no general Idaho law provisions governing privacy and security requirements regarding data storage. Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), files, documents, images, or data containing a student's educational record that are stored in or transmitted through a cloud computing service are defined as "student data" subject to the law's requirements (Idaho Code § 33-133(1)(j)(i)(12); see Section I.E.2.).

5. Access & Correction –

Insurance and health provisions: Idaho insurance laws and regulations governing the privacy of nonpublic personal information of consumers contain provisions regarding access and correction of such information (see Section I.E.7..). In addition, provisions of Idaho law governing specific types of health care facilities and providers and health data contain requirements regarding access and correction of such data (see Section I.D.9.). Finally, laws governing children's mental health services contain specific requirements regarding access to and correction of treatment records (see Section I.D.12.).

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), the Department of Education is required to develop policies for school districts and public charter schools governing access to and correction of student data (see Section I.E.2.).

Access and correction of records subject to Public Records Act: A person whose information is contained in a record otherwise subject to the Public Records Act's restrictions on disclosure may generally access such records and request correction of inaccurate items under specified statutory conditions (see Section I.C.10.).

6. Data Security –

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), the Department of Education is required to develop policies for school districts and public charter schools governing the security of student data (see Section I.E.2.).

Managed care programs: All managed care programs performing utilization management must adopt procedures designed to protect the confidentiality of patient health records. The law restricts recordings of telephone conversations in the course of requesting medical information only in compliance with state and federal law and with patient notification of the recording (Idaho Code § 41-3930(1)(d)).

7. Data Disposal –

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), the Department of Education is required to develop policies for school districts and public charter schools governing the security of student data that include data retention and disposition policies (see Section I.E.2.).

8. Data Breach –

Idaho's data breach notification law (Idaho Code § 28-51-104 through Idaho Code § 28-51-107) outlines the procedures that agencies, individuals, and commercial entities must follow in providing notice of a data breach to Idaho residents. The requirements are outlined in detail below.

Primary definitions: A "breach of the security of the system" is the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual, or commercial entity. Good faith acquisition of personal information by an employee or agent of an agency, individual, or commercial entity for the purposes of the agency, individual, or entity is not considered a breach of the security of the system, provided the information is not used or subject to further unauthorized disclosure (Idaho Code § 28-51-104(2)). A "commercial entity" is defined as a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, or any other legal entity, whether for profit or not for profit (Idaho Code § 28-51-104(3)).

"Personal information" is defined as an Idaho resident's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted:

- social security number;
- driver's license number or Idaho ID card number; or
- account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media (Idaho Code § 28-51-104(5)).

The term "primary regulator," for commercial entities or individuals licensed or chartered by the United States, is the entity's or individual's primary federal regulator. For individuals or entities licensed at the state level, the primary regulator is the Department of Finance for licensees of that department, the Department of Insurance for licensees of that department, and the Attorney General for all agencies and all other licensees (Idaho Code § 28-51-104(6)).

Notification requirement: A city, county, or state agency, an individual, or a commercial entity conducting business in Idaho and owning or licensing computerized data that includes personal information about Idaho residents must, on becoming aware of a breach of security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the agency, individual, or commercial entity must give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement (see below) and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system (Idaho Code § 28-51-105(1)). In addition, an agency, individual, or commercial entity that maintains computerized data containing personal information that it does not own or license must give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information of an Idaho resident has occurred or is likely to occur. Cooperation includes sharing information relevant to the breach with the owner or licensee (Idaho Code § 28-51-105(2)).

If an agency becomes aware of a breach of the security of the system, it must, within 24 hours of discovery, notify the Attorney General of the breach. This requirement does not relieve any agency of its obligation to report a security breach to the Office of the Chief Information Officer of the Department of Administration under Idaho technology authority policies (Idaho Code § 28-51-105(1), second paragraph).

Notice required as outlined above may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Notice must be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation (Idaho Code § 28-51-105(3)).

Form and content of notice: The required notice as outlined above includes written notice, telephonic notice, electronic notice if consistent with federal provisions regarding electronic records and signatures, or substitute notice (Idaho Code § 28-51-104(4)). Substitute notice is allowed if the agency, individual, or commercial entity demonstrates that the cost of providing notice would exceed $25,000; the number of Idaho residents to be notified exceeds 50,000; or the agency, individual, or commercial entity does not have sufficient contact information. Substitute notice consists of any two of the following:

- e-mail notice if the agency, individual, or commercial entity has e-mail addresses for the members of the affected Idaho residents;
- conspicuous posting of the notice on the agency's, individual's, or entity's website if one is maintained; and
- notice to major statewide media (Idaho Code § 28-51-104(4)(d)).

Exceptions: An agency, individual, or commercial entity that maintains its own notice procedures as part of an information privacy or security policy for the treatment of personal information that are otherwise consistent with the timing requirements of the breach notification law outlined above is deemed to be in compliance if the individual or entity notifies affected Idaho residents in accordance with its policies in the event of a breach of the security of the system (Idaho Code § 28-51-106(1)). An individual or commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance if the individual or commercial entity complies with such maintained procedures when a breach occurs (Idaho Code § 28-51-106(2)).

Violations: A violation of the data breach notification requirements may be enforced in a civil action by the primary regulator of an agency, individual, or commercial entity seeking injunctive relief and fines (see Section II.C.).

Criminal penalties applicable to governmental employees: Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor punishable by a fine of not more than $2,000, imprisonment for up to one year, or both (Idaho Code § 28-51-105(1), third paragraph).

9. Data Transfer & Cloud Computing –

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), files, documents, images, or data containing a student's educational record that are stored in or transmitted through a cloud computing service are defined as "student data" subject to the law's requirements (Idaho Code § 33-133(1)(j)(i)(12); see Section I.E.2.).

10. Other Provisions –

Public Records Act provisions: In general, any person has the right to examine and copy any public record under the state's Public Records Act (Idaho Code § 74-102). However, the law provides for exceptions to disclosures of such information, as outlined below.

Exemptions in state or federal law or court rules: Any public record exempt from disclosure under federal or state law or federal regulations is exempt from disclosure under the Public Records Act (Idaho Code § 74-104(1)). In addition, records contained in court files of judicial proceedings that may not be disclosed under rules of the Idaho Supreme Court also are generally exempt to the extent that confidentiality is provided by the rules, except that the exemption does not apply to

the extent that the records are necessary for a background check required by federal law regulating the sale of firearms, guns, or ammunition (Idaho Code § 74-104(2)).

Law enforcement and investigatory records: Specified investigatory records of law enforcement agencies, juvenile records, Department of Corrections records, records related to emergency response plans, and criminal history records are exempt from disclosure under the Public Records Act. The law specifies the circumstances under which such records must be kept confidential and exceptions under which they may be released (Idaho Code § 74-105).

Nothing in the Public Records Act may be construed to require disclosure of investigatory records compiled for law enforcement purposes by a law enforcement agency, but such exemption only applies to the extent that production of such records would interfere with enforcement proceedings, deprive a person of a right to a fair trial or impartial adjudication, constitute an unwarranted invasion of privacy, disclose the identity of a confidential source, disclose investigative techniques or procedures, endanger the life and physical safety of law enforcement personnel, or disclose the identity of a reporting party (Idaho Code § 74-124(1)). Persons involved in a motor vehicle collision are entitled to a copy of an impact report (Idaho Code § 74-124(2)). Inactive investigatory reports must be disclosed unless one of the exceptions outlined above applies (Idaho Code § 74-124(3)). The law specifies methods by which courts may require the disclosure of investigative records (Idaho Code § 74-124(4)).

Personnel records, health records, and other records containing personal information: The following types of records are specifically exempt from disclosure under the Public Records Act, among others:

- all personnel records of a current, former, or retired public official other than the official's public service or employment history or other specified salary or classification information; any other information in such records may not be disclosed without the subject's consent (Idaho Code § 74-106(1)-(2));
- information submitted to the state lottery for background check purposes (Idaho Code § 74-106(3);
- specified financial records of a personal nature, including bank records and records regarding security interest ownership (Idaho Code § 74-106(4));
- records of a personal nature related to applications for public care (Idaho Code § 74-106(6));
- employment security information as provided by law (Idaho Code § 74-106(7));
- personal records other than name, business address, and business phone related to a public agency pursuant to a licensing, registration, permit, or bond requirement of an inquiry into a person's fitness for such licensing or registration (Idaho Code § 74-106(8)-(9));
- records identifying a person infected with a reportable disease (Idaho Code § 74-106(12));
- records of hospital care, medical records (including prescriptions), and records of psychiatric care or professional counseling, to the extent that such records are not required for a background check required by federal law regulating the sale of firearms, guns, or ammunition (Idaho Code § 74-106(13));
- personal information from motor vehicle and driver records otherwise exempt (Idaho Code § 74-106(15));
- records associated with the state's trauma registry (Idaho Code § 74-106(23)) and health care directive registry (Idaho Code § 74-106(26); and
- residential street addresses and phone numbers of eligible law enforcement officers (Idaho Code § 74-106(30).

Other exempt items: A number of other types of documents are exempt from disclosure, including trade secrets, production records, and proprietary information (Idaho Code § 74-107); specified archaeological and library records (Idaho Code § 74-108); draft legislation, tax commission audit, and clean water trust find records (Idaho Code § 74-109); records of court proceedings regarding judicial authorization of abortion procedures on minors (Idaho Code § 74-110); and records related to the Uniform Securities Act (Idaho Code § 74-111).

Access to records of a person by a person: A person may inspect and copy the record of a public agency pertaining to that person even if the record is otherwise exempt from public disclosure (Idaho Code § 74-113(1)). A person may request an amendment of any record pertaining to him, and within 10 days of receiving such a request, a public agency must make the correction or inform the person in writing of the reasons it will not do so, as well as the person's right to appeal (Idaho Code § 74-113(2)). The right to inspect and amend does not include specified items, such as investigatory records in an ongoing investigation, information compiled in anticipation of a civil action, information related to adoption records, information otherwise exempt by statute or court rule, or certain prisoner records (Idaho Code § 74-113(3)).

The law provides for enforcement provisions regarding the right of access (Idaho Code § 74-115). The court may order a public official to disclose a public record or show cause why it should not do so. If the court finds that an official's decision not to disclose is not justified, it must order the disclosure, and if it finds that the decision was justified, it must return the item to the official without making a disclosure. In either case, the court must award reasonable attorney fees and costs to the prevailing party, if it finds that the request or refusal to provide records was frivolously pursued (Idaho Code § 74-116; see also Idaho Code § 74-113(2)). Finally, if the court finds that a public official has deliberately and in bad faith improperly refused a legitimate request for inspection and copying, a civil penalty must be assessed against the official not to exceed $1,000 (Idaho Code § 74-117).

D. Specific Types of Data

1. Biometric Data –

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), a student's biometric record is included in the definition of "personally identifiable data," personally identifiable student data," or "personally identifiable information" subject to the law's requirements (Idaho Code § 33-133(1)(h)). In addition, student biometric information may not be included in a student's educational record for purposes of the law's provisions (Idaho Code § 33-133(1)(j)(ii)(4)). Information collected pursuant to a statewide assessment via affective computing, including analysis of facial expressions, EEG brain wave patterns, pulse, blood volume, psychological measures, and other items, also may not be included in an educational record, except for special needs and exceptional students (Idaho Code § 33-133(1)(j)(ii)(8)). For more information on the SDATAA, see Section I.E.2.

2. Consumer Data –

Data breach notification requirements: Consumer data such as an Idaho resident's name, in combination with specified data elements when either the name or the data elements are not encrypted, is considered to be "personal information" subject to the provisions of the data breach notification law (Idaho Code § 28-51-104(5); see Section I.C.8.).

Identity theft: For purposes of Idaho laws prohibiting identity theft, a person's name, address, or telephone number is included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

3. Credit Card Data –

Limitations on information on payment card receipts: A merchant who accepts a payment card for the transaction of business may not print more than the last five digits of the payment card's account number or print the payment card's expiration date on a receipt provided to the cardholder. The prohibition does not apply to a transaction in which the sole means of recording the payment card account number or expiration date is by handwriting or an imprint or copy of the card (Idaho Code § 28-51-103(2)). For purposes of the prohibition, a "payment card" is defined as a credit card, charge card, debit card, or other card issued to a cardholder that allows the cardholder to obtain, purchase, or receive goods, services, money, or anything else of value from a merchant (Idaho Code § 28-51-103(1)(c)).

Merchants violating the provisions outlined above are subject to a civil penalty of not more than $250 for a first violation and $1,000 for second and subsequent violations. An action to recover the penalty may be brought by a prosecuting attorney, but if the prosecuting attorney does not bring such an action within 60 days of the date the violation is reported by the cardholder, the cardholder may bring the action. The penalties above are in addition to any remedies available to the cardholder. The penalty is paid into the state's general fund, not to the cardholder, but attorney fees are available to the party successfully bringing the action (Idaho Code § 28-51-103(3)).

Data breach notification requirements: A credit or debit card number, in combination with an Idaho resident's name and any required security code, access code, or password that would permit access to the resident's financial accounts, is considered to be "personal information" subject to the provisions of the state's data breach notification law, provided either the name or the number is not encrypted (Idaho Code § 28-51-104(5)(c)); see Section I.C.8.).

Identity theft: For purposes of Idaho laws prohibiting identity theft, a person's financial transaction card number is included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

4. Credit Reports –

Security freezes: Consumers may elect to place a security freeze on their files by making a request to a consumer reporting agency (CRA) under specified provisions of Idaho law, as outlined below.

> ***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.*

Requesting security freeze: A consumer may place a security freeze on the consumer's credit report by making a request in writing to a CRA by regular or certified mail at an address designated by the CRA, providing proper identification, and paying the required fee (Idaho Code § 28-52-103(1)). Within three business days of receiving the request, the CRA must place the freeze, and within five business days of receiving the request, the CRA must send written confirmation of the freeze to the consumer, together with a unique personal ID number or password to be used by the consumer when providing authorization for removal or temporary lifts of the freeze (Idaho Code § 28-52-103(2)). If a freeze is in place, a report or information may not be distributed to a third party without the prior express authorization of the consumer (Idaho Code § 28-52-103(3)). However, the CRA may communicate to a third party that a security freeze is in effect on the consumer's credit report. If a third party requesting a credit report in connection with a consumer's application for credit is notified of the existence of a freeze as outlined above, the third party may treat the application as incomplete (Idaho Code § 28-52-103(4)). The CRA must require proper identification from a consumer requesting to place, remove, or temporarily remove a security freeze (Idaho Code § 28-52-103(5)). In addition, the CRA must develop a contact method to receive and process a consumer's request to permanently remove or temporarily lift a freeze, including a postal address; an electronic contact method chosen by the CRA that may include the use of fax, Internet, or other electronic means; or the use of a telephone that is consistent with federal requirements placed on the CRA. In addition, the CRA must develop a secure electronic method for a consumer to request temporary lifting of a freeze (Idaho Code § 28-52-103(6)). Freezes may only be removed as outlined below (Idaho Code § 28-52-103(7)).

Removal and temporary lifting: A CRA may remove a security freeze only if the CRA receives the consumer's request through a contact method outlined above, together with proper identification and other information sufficient to identify the consumer, including the consumer's personal ID number or password, or if the consumer makes a material misrepresentation of fact in connection with the placement of the freeze and the CRA notifies the consumer in writing before removing the freeze (Idaho Code § 28-52-104(1)). The CRA must temporarily lift a security freeze on receipt of a consumer's request through a contact method outlined above, together with proper identification and other information sufficient to identify the consumer, the consumer's personal ID number or password, the proper information concerning the third party who is to receive the report or the time period for which the report is to be available, and any applicable fee (Idaho Code § 28-52-104(2)).

The freeze must be removed or temporarily lifted within three business days after the business day on which the CRA receives the written request using a contact method other than a secure electronic method as outlined above (Idaho Code

§ 28-52-104(3)(a)). A freeze must be temporarily lifted by the CRA within 15 minutes of receipt of a request through the secure electronic contact method chosen by the CRA, if the request is received between 6:00 AM and 9:00 PM mountain time (Idaho Code § 28-52-104(3)(b)). The CRA need not remove or temporarily lift a security freeze within these time frames if the consumer fails to meet the requirements regarding proper identification, the entities or periods applicable to a temporary lifting, or applicable fee payments, or if the CRA's ability to remove the freeze is prevented by an act of God, unauthorized illegal activity of a third party, operational interruption, governmental action, regularly scheduled maintenance, reasonable maintenance that is unexpected or unscheduled, or receipt of a removal request outside normal business hours (Idaho Code § 28-52-104(4)).

Exceptions: A CRA may furnish a copy of a consumer's credit report to a third party if the purpose of the report is to use the report for purposes permitted under the federal Fair Credit Reporting Act (FCRA); review the consumer's report with a third party, including for account maintenance or monitoring credit line increases or other upgrades; collect a financial obligation owed by the consumer to a third party requesting the report; or review the consumer's account with another person, or collect on a financial obligation owed by the consumer to another person and the request is for purposes permitted under the FCRA or the third party is a subsidiary, affiliate, agent, assignee, or prospective assignee of the person holding the consumer's account or to whom the consumer owes a financial obligation (Idaho Code § 28-52-105(1)).

Additional exceptions apply to specified disclosures, including disclosures where the third party does not use the credit report for the purposes of serving as a factor in establishing a consumer's eligibility for credit; the third party is acting under a court order, warrant, or subpoena requiring a release; the third party is a child support agency or the federal Department of Health and Human Resources under specified conditions; the purpose of the report is to investigate delineated taxes, assessments, or unpaid court orders; the third party is using the information solely for criminal record information, tenant screening, employment screening, fraud prevention or detection, or personal loss history information; the third party is a person or entity regulated under Idaho insurance law; the third party is administering a credit file monitoring subscription service; or the third party requests the report for the sole purpose of providing the consumer with a copy of the consumer's credit report or credit score at the consumer's request (Idaho Code § 28-52-105(2)).

The security freeze law does not apply to CRAs that act only as a reseller of credit information by assembling information held and maintained in the databases of another or multiple CRAs and that do not maintain a permanent database of information from which new credit reports are produced, as well as specified check service or fraud prevention service companies and deposit account information service companies (Idaho Code § 28-52-105(3)). Finally, no person is prohibited from obtaining, aggregating, or using information lawfully obtained from public records in a manner that does not otherwise violate the security freeze provisions (Idaho Code § 28-52-105(4)).

Fees: In general, a fee may not be charged for the first placement of a security freeze during a 12-month period and for the first temporary lift of a freeze within such period. CRAs may charge a fee of up to $6.00 to a consumer for the second and subsequent placement, or second or subsequent temporary lift, of a freeze during a 12-month period (Idaho Code § 28-52-106(1)). CRAs may not charge a fee for the placement of any freeze to a consumer who has been the victim of identity theft and who submits a valid police report or investigative report or complaint that the consumer has filed with a law enforcement agency (Idaho Code § 28-52-106(2)). A fee of up to $10 may be charged if a consumer fails to retain his original personal ID number or password provided by the CRA and the consumer requests reissuance or replacement of the ID number or password (Idaho Code § 28-52-106(3)).

Changes in report subject to freeze: If a security freeze is in place, a CRA must notify the consumer within 30 days if the CRA changes the consumer's name, date of birth, social security number, or address. The CRA may make technical modifications to information in a credit report, such as the addition or subtraction of abbreviations to names and addresses and transposition or corrections of incorrect numbering or spelling. If an address change is made, confirmation must be sent to the new and former address of the consumer (Idaho Code § 28-52-107).

Enforcement: A CRA that willfully or negligently fails to comply with any requirement imposed by the security freeze law with respect to any consumer is liable to the consumer in a civil action, and a person obtaining information under false pretenses is liable to the CRA for damages, as well (see Section I.G.1.). In addition, the Attorney General may enforce the provisions of the security freeze law and has exclusive jurisdiction with respect to violations involving the failure of a CRA to temporarily lift a security freeze within 15 minutes (see Section II.C.).

5. Criminal Records –

Accuracy, security, and disclosure of criminal history records: The Idaho State Police (hereinafter "the Department") must adopt reasonable procedures to ensure that criminal justice information is accurate and complete, notify criminal justice agencies or persons known to have received information of a material information that is inaccurate or incomplete, provide adequate procedures to protect such information from unauthorized access or accidental or deliberate damage, and provide procedures for screening, supervising, and disciplining Department personnel to minimize the risk of security violations (Idaho Code § 67-3007(1)). The Department also must establish procedures for persons to review and challenge the accuracy and completeness of Idaho criminal history records pertaining to them, including provisions for administrative review and necessary corrections (Idaho Code § 67-3007(2)). The Department has promulgated regulations as outlined above to govern the transmittal of criminal history records and procedures for contesting their accuracy and completeness (Idaho Regs. 11.10.02.000 through Idaho Regs. 11.10.02.032).

The Department is immune from any liability arising from the accuracy or completeness of records it receives from the FBI or another state central repository if the Department acts in good faith (Idaho Code § 67-3007(5)).

The Department is required to provide copies of or communicate information from criminal history records to the following:

- criminal justice agencies and the courts; and
- a person or public or private agency, on written application on a Department-approved form, subject to the following:
    - A request must be submitted in writing or as provided by rule, but an in-person request is allowed by the record subject;
    - The request must specify a person by name and date of birth, and fingerprints may be required to establish positive identification;
    - Responding to the request does not interfere with the secure and orderly conduct of the Department and does not substantially prejudice its functions;
    - A record of an arrest that does not contain a disposition after 12 months from the date of arrest may only be disseminated to criminal justice agencies, to the subject, or to a person requesting the information with a signed release from the subject; and
    - Any release of criminal history information must prominently display the following statement: "AN ARREST WITHOUT DISPOSITION IS NOT AN INDICATION OF GUILT" (Idaho Code § 67-3008(2)).

Access provided as outlined above does not create a duty on a person, employer, private agency, or public agency to examine a criminal history record of an employee, applicant, or volunteer (Idaho Code 67-3008(5)). A person, private agency, or public agency may not disseminate criminal history information obtained from the Department to a person or agency that is not a criminal justice agency or a court without a signed release from the subject (Idaho Code § 67-3008(6)).

It is a misdemeanor for a person, for personal gain, to request, obtain, or attempt to obtain criminal history records under false pretenses or willfully communicate or attempt to communicate criminal history records to any agency or person not authorized to receive the information (Idaho Code § 67-3009(1)). In addition, it is unlawful to willfully solicit, accept, or agree to accept from another any pecuniary benefit as consideration either for willfully falsifying criminal history records or willfully requesting, obtaining, or seeking to obtain such records for an unauthorized purpose. A violation of this provision is a felony subject to a fine of up to $10,000 and imprisonment for up to five years (Idaho Code § 67-3009(2)).

Guide to lawful applications and interviews: For information on guidance from the Idaho Department of Labor and the Idaho Human Rights Commission concerning the conduct of lawful employment applicants and interviews, including inquiries about criminal records, see Section I.E.6.

Required background screening and criminal history records checks: gobble Specified inquiries into criminal history and records are required for certain positions, including physicians seeking expedited licensure under the Medical Practice Act (Idaho Code § 54-1847); applicants for licensing as a registered or licensed practical nurse under the Interstate Nurse

Licensure Compact (Idaho Code § 54-1418) and the Advanced Practice Register Nurse Compact (Idaho Code § 54-1419); applicants for licensure under the EMS Personnel Licensure Interstate Compact (Idaho Code § 56-1013E); owners, operators, and employees of daycare facilities (Idaho Code § 39-1105) and children's residential care facilities (Idaho Code § 39-1210); foster parents (Idaho Code § 39-1211); applicants for public adjuster insurance licenses (Idaho Code § 41-5805); school district employees (Idaho Code § 33-130); and mortgage brokers and lenders (Idaho Code § 26-31-103), among many others.

Public Records Act provisions: Specified investigatory records of law enforcement agencies, juvenile records, Department of Corrections records, and criminal history records are exempt from disclosure under the Public Records Act (see Section I.C.10.).

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), a student's juvenile delinquency records and criminal records generally may not be included in a student's educational record for purposes of the law's provisions unless otherwise required by the law (Idaho Code § 33-133(1)(j)(ii)(1)). For more information on the SDATAA, see Section I.E.2.

6. Drivers' Licenses/Motor Vehicle Records –

Release and use of personal information in motor vehicle and driver records: In general, the Idaho Transportation Department and its officers and employees may not knowingly disclose to any person or entity personal information about any individual when such information was obtained from a motor vehicle or driver record (Idaho Code § 49-203(1)). Certain disclosures are permitted, including those for use in connection with statutorily prescribed purposes such as motor vehicle or driver safety and theft, emissions, product alterations, recalls and advisories, and other purposes necessary to carry out the purposes of federal law (Idaho Code § 49-203(2)). Information also may be disclosed if the person requesting it demonstrates to the Department that it has the written consent of the data subject (Idaho Code § 49-203(3)).

On proof of the identity of the person requesting a record, personal information may also be disclosed for the following purposes:

- for use by a government agency, or a private person acting on the agency's behalf, in carrying out its functions;
- for use in connection with statutorily prescribed purposes such as motor vehicle or driver safety and theft, emissions, product alterations, recalls and advisories, market research, and other purposes;
- for use in the normal course of business by a legitimate business or its employees or agents to verify the accuracy of personal information submitted to it and, if such information is not correct or no longer correct, to obtain the correct information, but only to prevent fraud through the pursuit of legal remedies;
- for use in connection with a civil, criminal, administrative, or arbitral proceeding as specified by law;
- for use in research activities and statistical reports, provided the personal information is not published, redisclosed, or used to contact individuals;
- for specified uses by insurers;
- for use in providing notice of towed or impounded vehicles;
- for use by an employer to verify information pertaining to commercial driver's license holders;
- for bulk distribution of surveys, marketing, or solicitations, where the Department has obtained the written consent of the data subject;
- for any other use specified by law related to public safety or motor vehicle operation; or
- for use in connection with private toll transportation facilities, including parking facilities, for specified purposes (Idaho Code § 49-203(4)).

Personal information in an individual's motor vehicle or driver record must be disclosed in response to a request for disclosure without regard to the intended use of the information if the Department has obtained the written consent of the data subject (Idaho Code § 49-203(5)).

An individual's photograph, digitized image of a photograph, digitized signature, social security number, and medical or history information may not be disclosed without the written consent of the data subject, except for use by a government entity in carrying out its functions or use in connection with civil, criminal, administrative, and arbitral proceedings as provided by law (Idaho Code § 49-203(6)).

Authorized recipients of personal information may redisseminate it only for one of the purposes outlined in the bulleted points above. The law defines who may be considered an "authorized recipient" (Idaho Code § 49-203(7)).

The Department is authorized to adopt rules to implement the disclosure requirements outlined above, but our research has revealed no such rules. All disclosures are subject to payment of applicable fees (Idaho Code § 49-203A).

Any person requesting disclosure of personal information from Department records who misrepresents his identity or makes a false statement to the Department on any required application is guilty of perjury (Idaho Code § 49-204).

Public Records Act provisions: Personal information from motor vehicle and driver records exempt from disclosure as outlined above also are exempt from disclosure under the Public Records Act (Idaho Code § 74-106(15)).

Data breach notification requirements: A driver's license number or Idaho ID card number, in combination with an Idaho resident's name, is considered to be "personal information" subject to the provisions of the state's data breach notification law, provided either the name or the number is not encrypted (Idaho Code § 28-51-104(5)(b)); see Section I.C.8.).

Identity theft: For purposes of Idaho laws prohibiting identity theft, a person's driver's license number is included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

7. Electronic Communications/Social Media Accounts –

Our research has revealed no Idaho law specifically addressing privacy and data security with respect to electronic communications or social media accounts. For information on laws governing interception of wire, oral, or electronic communications, see Section I.F.. For information on anti-spam laws restricting the sending of bulk e-mail advertisements, see Section I.E.1..

8. Financial Information –

Data breach notification requirements: An account number, in combination with an Idaho resident's name and any required security code, access code, or password that would permit access to the resident's financial accounts, is considered to be "personal information" subject to the provisions of the state's data breach notification law, provided either the name or the number is not encrypted (Idaho Code § 28-51-104(5)(c)); see Section I.C.8.).

Identity theft: For purposes of Idaho laws prohibiting identity theft, a checking or savings account number, or any other numbers or information that can be used to access a person's financial resources, are included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

Public Records Act provisions: Specified financial records are exempt from disclosure under the Public Records Act (see Section I.C.10.).

Insurance law on privacy of consumer information: For information on statutory and regulatory requirements applicable to the collection, disclosure, and use of nonpublic personal consumer financial information, see Section I.E.7..

9. Health Data –

Mental health records: Patients of public or private hospitals, sanatoria, mental health centers, or other institutions to provide care and treatment for the mentally ill have the right to have reasonable access to all records concerning the patient (Idaho Code § 66-346(a)(7)). The right may be denied by a facility director, who must document the reasons for the denial in the patient's treatment record (Idaho Code § 66-346(c)).

All records made for the purpose of the law governing the hospitalization of the mentally ill and directly or indirectly identifying a patient or former patient or an individual whose involuntary assessment, detention, or commitment is being sought must be kept subject to disclosure under the Public Records Act. Such records also may be disclosed to any person if the individual identified or his attorney or legal guardian consents to the disclosure, the disclosure is necessary to carry out the provisions of the law, or a court directs that disclosure is necessary and failure to disclose is contrary to the public interest (Idaho Code § 66-348).

An agent of the patient has the same rights as the patient to access records and to authorize disclosure as outlined above (Idaho Code § 66-606).

For information on confidentiality requirements regarding records relating to children's mental health services, see Section I.D.12.

Physicians: Physicians, physician assistants, interns, and residents are subject to discipline by the Board of Medicine for failure to safeguard the confidentiality of medical records or other information pertaining to identifiable patients (Idaho Code § 54-1814(13)). In any such disciplinary action, the Board may, among other penalties, suspend, limit, or revoke a physician's license and may impose an administrative penalty of up to $10,000 (Idaho Code § 54-1806A(9)).

Pharmacists: All prescriptions, drug orders, records, or other prescription information specifically identifying an individual patient must be held in the strictest confidence. No person in possession of such information may release it, except as requested by a number of persons and entities, including the Board of Pharmacy, the patient or a representative regarding the patient's own records, a practitioner who issued the prescription or his designee, specified state and federal agencies, and insurers (Idaho Code § 54-1727(1)). Pharmacists may provide aggregate data that does not identify a patient to qualified researchers (Idaho Code § 54-1727(2)). Persons having knowledge of a prescription, drug order, or pharmacy-related information by virtue of their office or occupation must not divulge the information except as authorized above, and persons to whom such information is divulged under these provisions may not redisclose the information except as authorized (Idaho Code § 54-1727(3)). The Board of Pharmacy has the authority to inspect pharmacy records, and courts have the authority to order release of such information after a showing of just cause. Any other board or agency also may inspect any records under its regulatory jurisdiction, whether or not the records contain information protected as outlined above (Idaho Code § 54-1727(4)).

Persons found to be in violation of these requirements are subject to an administrative penalty of not more than $3,000 per violation (Idaho Code § 54-1727(5)). However, no person is liable for any loss or damage based on a good faith release of records (Idaho Code § 54-1727(6)).

Residential care and assisted living records: Records required for admission to a residential care or assisted living facility must be maintained and updated for administrative purposes only and are confidential. Such records generally are available only to administration, professional consultants, the resident's physician or authorized provider, and representatives of the licensing agency. The law specifies the items to be included in such records (Idaho Code § 39-3315). In addition, residents of such facilities have the right to confidentiality of all personal and clinical records (Idaho Code § 39-3316(9)).

Acupuncture: The State Board of Acupuncturists may refuse to issue or renew, or may suspend or revoke, the license of an acupuncturist who fails to maintain the confidentiality of records or other information pertaining to an identifiable client (Idaho Code § 54-4711(4)).

Chiropractors: The State Board of Chiropractic Physicians may restrict, suspend, or revoke the license of a chiropractor who fails to safeguard the confidentiality of chiropractic records or other information pertaining to an identifiable client (**Idaho Code § 54-712(7)**). The law provides for the imposition of such discipline (Idaho Code § 54-713) and specifies that a chiropractor found in violation may be subject to an administrative fine of up to $2,000 (Idaho Code § 54-713(1)(f)).

Managed care programs: All managed care programs performing utilization management must adopt procedures designed to protect the confidentiality of patient health records. The law restricts recordings of telephone conversations in the course of requesting medical information only in compliance with state and federal law and with patient notification of the recording (Idaho Code § 41-3930(1)(d)).

Cancer registry: The Department of Health and Welfare or its authorized contractor must take measures to ensure that all identifiable information in its possession through the operation of the state's central cancer registry is kept confidential. The Department or contractor may enter into agreements to exchange confidential information with other states' registries to obtain complete reports of Idaho residents or to provide information to other registries on patients treated in Idaho, and may provide such information to other registries, federal cancer control programs, or researchers to collaborate on research studies (Idaho Code § 57-1706).

No action may be brought against reporting entities or their employees who participate in the cancer registry program in good faith (Idaho Code § 57-1707(1)). In addition, the license of a facility or health care provider may not be denied, suspended, or revoked for the good faith disclosure of confidential or privileged information in accordance with program requirements (Idaho Code § 57-1707(2)). However, such immunity does not apply to disclosures made due to gross negligence or willful misconduct of the reporting entity (Idaho Code § 57-1707(3)).

HIV/AIDS and venereal diseases: Reports containing patient identification that are submitted to the Department of Health and Welfare under requirements regarding the reporting of venereal diseases, including HIV/AIDS, may only be used by public officials authorized to conduct patient investigations and generally are not subject to public inspection. Any person who willfully or maliciously discloses such information to any third party, except pursuant to written authorization by the data subject, is guilty of a misdemeanor (Idaho Code § 39-606).

A state or local health authority may contact persons who, in the authority's judgment, have been exposed to HIV or hepatitis B (Idaho Code § 39-610(2)). HIV-related information also may be disclosed to other state or local health agencies when necessary to carry out the duties of the agency in the investigation, control, and surveillance of disease (Idaho Code § 39-610(4)).

Public Records Act provisions: Specified health records are exempt from disclosure under the Public Records Act (see Section I.C.10.).

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), a student's medical or health records may not be included in a student's educational record for purposes of the law's provisions (Idaho Code § 33-133(1)(j)(ii)(2)). Information collected pursuant to a statewide assessment via affective computing, including analysis of facial expressions, EEG brain wave patterns, pulse, blood volume, psychological measures, and other items, also may not be included in an educational record, except for special needs and exceptional students (Idaho Code § 33-133(1)(j)(ii)(8)). For more information on the SDATAA, see Section I.E.2.

10. Social Security Numbers –

Disclosure of SSNs: Under a specific provision of the Credit Report Protection Act, except as otherwise specifically provided by law, no person may intentionally communicate an individual's social security number (SSN) to the general public (Idaho Code § 28-52-108(1)).

Data breach notification requirements: An SSN, in combination with an Idaho resident's name, is considered to be "personal information" subject to the provisions of the state's data breach notification law, provided either the name or the number is not encrypted (Idaho Code § 28-51-104(5)(a)); see Section I.C.8.).

SDATAA: Under the state's Student Data Accessibility, Transparency and Accountability Act (SDATAA), a student's SSN is included in the definition of "personally identifiable data," "personally identifiable student data," or "personally identifiable information" subject to the law's requirements (Idaho Code § 33-133(1)(h)). In addition, a student's SSN may not be included in a student's educational record for purposes of the law's provisions (Idaho Code § 33-133(1)(j)(ii)(3)). For more information on the SDATAA, see Section I.E.2.

Identity theft: For purposes of Idaho laws prohibiting identity theft, a person's SSN is included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

11. Usernames & Passwords –

Data breach notification requirements: An account number, or credit or debit card number, in combination with an Idaho resident's name and any required security code, access code, or password that would permit access to the resident's

financial accounts, is considered to be "personal information" subject to the provisions of the state's data breach notification law, provided either the name or the number is not encrypted (Idaho Code § 28-51-104(5)(c)); seeSection I.C.8.).

Identity theft: For purposes of Idaho laws prohibiting identity theft, a person's personal identification code is included in the types of identifying information subject to the prohibition (Idaho Code § 18-3122(10); see Section I.G.2.).

Credit freezes: For information on passwords required to be provided and used for the removal or temporary lifting of a security freeze on a consumer credit report, see Section I.D.4.

12. Information about Minors –

Children's mental health services: Records directly or indirectly identifying a patient or former patient or an individual whose involuntary commitment has been sought under law provisions governing children's mental health services must be kept confidential and may not be disclosed to any person except with the consent of the person identified or a legal guardian, or as necessary to carry out provisions of the law (Idaho Code § 16-2428, first paragraph). No person in possession of confidential statements made by a child over the age of 14 in the course of treatment may disclose the information to the child's parent or others without the written permission of the child, except where necessary for insurance coverage, to carry out a treatment plan or prevent harm to the child or others, or unless authorized by court order (Idaho Code § 16-2428(1)). A child has the right to access information regarding his treatment, to obtain copies of records, and to submit clarifying or correcting documents of reasonable length for inclusion in the record (Idaho Code § 16-2428(2)). Access to a child may be denied when a physician or other mental health professional believes and notes in the child's record that disclosure would be damaging to the child (Idaho Code § 16-2428(3)).

Abortions: In general, written consent from a parent or guardian is required for the performance of an abortion procedure on an unemancipated minor (Idaho Code § 18-609A(1)). A judge may authorize an abortion on a finding that the minor is mature and capable of giving informed consent, or the procedure would be in the minor's best interest (Idaho Code § 18-609A(2)). The law provides for procedures to be followed in court proceedings for judicial authorization (Idaho Code § 18-609A(3)-(6)). Parental consent or judicial authorization is not required if the minor certifies that the pregnancy resulted from a rape or sexual conduct with the minor by the minor's parent, stepparent, uncle, grandparent, sibling, adoptive parent, legal guardian, or foster parent, or where a medical emergency exists and the attending physician records the symptoms and diagnosis on which the judgment was made on the minor's medical record (Idaho Code § 18-609A(7)).

Drug treatment: If a person seeking treatment or rehabilitation for addiction or dependency to any drug is age 16 or older, the fact that the person sought treatment or rehabilitation or that he is receiving such services must not be reported or disclosed to the parents or legal guardian of the person without his consent. However, such persons must be counseled as to the benefits of involving the person's parents or legal guardian in treatment or rehabilitation (Idaho Code § 37-3102).

Access to records by divorced parents: Access to records pertaining to a minor child, including medical, dental, health, and school or educational records, may not be denied to a noncustodial parent. However, information concerning the minor child's address must be deleted from records provided to a noncustodial parent if the custodial parent has advised the records custodian in writing to do so (Idaho Code § 32-717A).

13. Location Data –

Our research has revealed no Idaho law specific to the privacy of location data.

14. Other Personal Data –

Address confidentiality for law enforcement officers: A public agency may not disclose to any person or entity the Idaho residential street address or telephone number of a law enforcement officer and such officer's residing household members on the submission of an application and fee by such an officer except if directed by court order, if requested by a law enforcement agency, if requested by a financial institution or title company for business purposes, or if the officer provides written permission for the disclosure (Idaho Code § 19-5802). The law provides for the application process to be followed by officers, and once an application and fee are received, the public agency must comply with the restrictions on disclosure for four years, after which the officer may renew the exemption with a new application and fee (Idaho Code § 19-5803(1)). Law enforcement officers also may submit an application requesting a public agency to use an alternative Idaho mailing address on all applications and on all identification cards, licenses, permits, tags, and other similar documents

issued to the officer or household members, and the public agency must comply with the request (Idaho Code § 19-5803(2)). Persons cease to be eligible for the exemption once they are no longer officers or household members. Within 30 days of this occurrence, the person must notify all public agencies to which the person made an application. If an officer changes employment but is still eligible for the exemption, he must submit a new application to every public agency to which the officer had previously made an application (Idaho Code § 19-5803(3)). Public agencies are not prohibited from obtaining the residential street address and telephone number of a law enforcement officer or household member, and an officer submitting an application as outlined above must provide such information to his employing entity (Idaho Code § 19-5803(4)).

No public agency or employee thereof, while acting within the course and scope of its employment and without malice or criminal intent, may be held liable in tort for any injury suffered from the release of confidential information under the above provisions (Idaho Code § 19-5804).

E. Sector-Specific Provisions

1. Advertising & Marketing –

Anti-spam law: Any person using an interactive computer service to initiate or cause the sending or transmittal of any bulk e-mail advertisement must provide an e-mail address readily identifiable in the advertisement to which the recipient may send a request declining to receive such e-mail (Idaho Code § 48-603E(2)). It is unlawful for any person who uses an interactive computer service to initiate or cause the sending or transmittal of any bulk e-mail advertisement to any recipient that the sender knows or has reason to know engages in any of the following:

- uses the name of a fictitious name or third party in the return address field without the permission of the third party;
- misrepresents any information in identifying the point of origin of the transmission path of the bulk e-mail;
- fails to contain information identifying such point of origin; or
- sends or transmits, at any time after five days after a declination, any bulk e-mail advertisement to a recipient who provided the sender with a request declining receipt of such advertisements (Idaho Code § 48-603E(3)).

Recipients of bulk e-mail advertisements sent in violation of the above requirements are entitled to bring a cause of action to recover damages (see Section I.G.1.). It should be noted, however, that the federal CAN-SPAM Act preempts state claims that are not based on traditional tort theories of falsity and deception (15 U.S.C. § 7707(b)(1)).

The anti-spam law does not apply to the following:

- a person, including an interactive computer service, who provides users with access to a computer network and who transmits e-mail as part of that service, unless the person transmits bulk e-mail advertisements on behalf of those persons that the person knows, or should have known, were transmitted in violation;
- e-mail advertisements accessed by the recipient from an electronic bulletin board;
- a person who provides users with access to e-mail at no charge, including receiving and transmitting bulk e-mail advertisements, and as a condition of access, requires users to receive unsolicited advertisements; and
- the transmission of bulk e-mail advertisements from an organization or similar entities to its members (Idaho Code § 48-603E(5)).

In addition, an interactive computer service is not liable for an action voluntarily taken in good faith to block or prevent the receipt or transmission through its service of any bulk e-mail advertisement that is reasonably believed to violate the anti-spam provisions (Idaho Code § 48-603E(6)).

Do-not-call: Idaho residential, mobile, or telephonic paging device subscribers wishing to be placed on the state's "no telephone solicitation contact" list may be placed on the list through procedures approved by the Attorney General (Idaho Code § 48-1003A(1)(a)). The national Do-Not-Call Registry established by the FTC may serve as the state's no telephone solicitation contact list (Idaho Code § 48-1003A(1)(b)). According to guidance issued by the Attorney General's consumer practice division, the state does not maintain its own list, and the Attorney General cannot register a consumer's telephone number on the national Do-Not-Call Registry, but it is unlawful for telephone solicitors to contact Idaho phone numbers registered on the national list. The Attorney General also notes that consumers may file complaints with the consumer protection division or the FTC if they receive unwanted telemarketing calls.

Breach notification requirements: Persons engaged in the advertising and marketing sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

2. Education –

SDATAA: The Student Data Accessibility, Transparency and Accountability Act (SDATAA; Idaho Code § 33-133) imposes requirements on the State Board of Education and school districts, including public charter schools, with respect to the collection, use, and disclosure of student information, as outlined below.

Primary definitions: For purposes of the SDATAA, "personally identifiable data," "personally identifiable student data," or "personally identifiable information" includes a student's name; the name of a student's parents or family members; addresses of a student or family members; personal identifiers such as a student's social security number, student education unique ID number, or biometric record; other indirect identifiers such as date of birth, place of birth, and mother's maiden name; and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community not having personal knowledge of the relevant circumstances to identify the student with reasonable certainty, or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates (Idaho Code § 33-133(1)(h)).

"Student data" is data collected or reported at the individual student level included in a student's educational record, including items such as state and national assessment results; courses taken and other transcript information; course grades and grade point average; date of birth, grade level, and expected graduation dates; degree, diploma, and other school exit information; attendance and mobility information; data required to calculate the federal four-year adjusted secondary cohort graduation rate; discipline reports; remediation information; demographic data and program participation information; and files, documents, images, or data containing a student's educational record that are stored in or transmitted through a cloud computing service (Idaho Code § 33-133(1)(j)(i)).

A "student educational record" is all information directly related to a student and recorded and kept in the data system. Daily assignments, homework, reports, chapter tests, and similar assessments or other school work considered to be daily or weekly work may not be included in a student's permanent educational record. A student educational record may include information considered to be personally identifiable (Idaho Code § 33-133(1)(k)). However, note that the law specifically prohibits the following items from being included in a student's educational record: juvenile delinquency records and criminal records; medical and health records; student social security numbers; student biometric information; gun ownership records; sexual orientation information; religious affiliation; and except for special needs and exceptional students, any data collected pursuant to a statewide assessment via affective computing, including specified information regarding facial analyses, EEG brain wave patterns, heart rate, pulse, and data measuring psychological resources or social skills, among others (Idaho Code § 33-133(1)(j)(ii)).

Administration: The Executive Office of the State Board of Education is responsible for implementing the provisions of the SDATAA and for making all decisions related to the collection and safeguarding of student data (Idaho Code § 33-133(2)).

Required policies: The Board must create, publish, and make available a data inventory and index of data elements with respect to student data and develop policies and procedures to comply with all relevant state and federal privacy laws, including Family Educational Rights and Privacy Act (FERPA) requirements. Such policies must include access restrictions, posting of interagency data sharing agreements, and criteria for approval of data requests from researchers and state agencies. The Board also must ensure that any contract entered into by the Board includes provisions requiring and

governing data destruction dates and specific restrictions on data use, and that all school districts, primary schools, secondary schools, and other institutions entering into a contract that governs databases, online services, assessments, special education, or instructional supports with private vendors include provisions regarding the use of student data as outlined by law (Idaho Code § 33-133(3)(a)-(b)).

The Board must develop a detailed security plan that includes guidelines for the student data system, including guidelines for authentication of authorized access, privacy compliance standards, privacy and security audits, breach planning, notification and procedures, and data retention and disposition policies (Idaho Code § 33-133(d)). In addition, the Board is responsible for ensuring routine and ongoing FERPA and SDATAA compliance; ensuring that contracts with private vendors include express security provisions, including penalties; and providing notices to the governor as required by law (Idaho Code § 33-133(3)(e)-(g)).

Transfers of confidential student information: Unless otherwise approved by the Board, any data deemed confidential may not be transferred to any federal, state, or local agency or other organization or entity outside of Idaho, unless one of the following exceptions is present:

- A student transfers out of the state, or a school or school district seeks help with locating an out-of-state transfer;
- A student leaves the state to attend an out-of-state education or training program;
- A student voluntarily participates in a program for which a data transfer is a condition or requirement for participation;
- The Board or the State Department of Education may share data with a vendor to the extent necessary as part of a contract that governs databases, online services, assessments, special education, or instruction supports with a vendor;
- Information is shared pursuant to an agreement between two school districts where a student transfers from an Idaho district abutting another state to the nearest appropriate district in the neighboring state; or
- A student is classified as a migrant for federal reporting purposes (Idaho Code § 33-133(3)(c)).

Miscellaneous provisions: The Board is charged by law with adopting rules to implement the SDATAA (Idaho Code § 33-133(4)). However, no such rules appear to have been adopted.

Unless otherwise prohibited by law or court order, school districts must provide parents or guardians with copies of all of their child's educational records, on request, if the child has not attained age 18 (Idaho Code § 33-133(6)).

The SDATAA requires the Board to develop a model policy for school districts and public charter schools that governs data collection, access, security, and use, and each school district and charter school must adopt the policy. [Note: The Board has adopted the model policy and made it available on its website.] Any district or public charter school that fails to adopt the policy where any inappropriate release of data occurs is liable for a civil penalty of up to $50,000 per violation, recoverable in a civil action by the Board, with the assistance of the Attorney General (Idaho Code § 33-133(7)).

Internet use policies: Each school district must file an acceptable Internet use policy with the State Superintendent of Public Instruction every five years. The policy must include provisions that, among other items, prohibit the use of school computers to transmit material harmful to minors, provide for computer filters to block access to obscene materials, and include components of Internet safety integrated into the district's instructional program. The policy also may require written parental permission for Internet use by minors and may differentiate acceptable uses among elementary, middle, and high school students (Idaho Code § 33-132).

Breach notification requirements: Persons engaged in the education sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

3. Electronic Commerce –

Breach notification requirements: Persons engaged in the electronic commerce sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

4. Financial Services –

Breach notification requirements: Persons engaged in the financial services sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

Insurance regulations on privacy of consumer information: For information on requirements applicable to insurers with respect to the collection, disclosure, and use of consumer financial and health information, see Section I.E.7.

5. Health Care –

Medical records and information: For information on laws addressing specified entities with respect to their obligations regarding patient access to medical records and restrictions on the disclosure of such records, see Section I.D.9.

Breach notification requirements: Persons engaged in the health care sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

6. HR & Employment –

Guide to lawful applications and interviews: The Idaho Department of Labor and the Idaho Human Rights Commission have issued a guide to lawful applications and interviews that outlines appropriate procedures to follow and questions to ask for employers in interviewing and hiring prospective applicants. The guide specifies, among other items, that while it is permissible for employers to ask if an applicant has ever been convicted of a crime, the question should be followed by an indication that a conviction does not operate as an automatic bar to employment. Employers should not ask whether applicants have been arrested or charged with a crime.

Blacklists and references: No employer may maintain a blacklist or notify any other employer that a current or former employee has been blacklisted by the employer for purposes of preventing the employee from obtaining employment (Idaho Code § 44-201(1)). However, an employer who in good faith provides information about job performance of a former or current employee at the request of the employee or of the prospective employer of that employee may not be held liable for the disclosure or the consequences of providing the information. Good faith is presumed unless there is a showing by clear and convincing evidence that the employer disclosed the information with actual malice or with deliberate intent to mislead. "Actual malice" means knowledge that the information was false or given with reckless disregard as to its falsehood (Idaho Code § 44-201(2)).

Drug-free workplace and employee assistance programs: Under the Employer Alcohol and Drug-Free Workplace Act (Idaho Code § 72-1701 et seq.), employers may participate in a voluntary program allowing them to conduct drug and alcohol testing of employees provided statutory requirements are met. All information, including reports and test results, written or otherwise, collected through such a program must be kept confidential and are intended for the employer's internal business use. Such information also may be used in a proceeding involving a workplace discharge for misconduct, disciplinary or rehabilitative actions based on positive tests, or false test result claims by employees, as required to be disclosed by federal Department of Transportation law or regulation or other federal law, or as required by service of legal process (Idaho Code § 72-1712(1)). Employers, laboratories, medical review officers, employee assistance programs, and drug and alcohol rehabilitation programs who receive or have access to such information generally must keep it confidential (Idaho Code § 72-1712(3)). However, employers may use such information in a lawful manner as provided under laws governing employee assistance programs (see below) (Idaho Code § 72-1712(4)).

No provider professionally licensed by the state and providing services to employee assistance program participants may disclose to an employer, and no employer may seek disclosure of, any communication from a participant privileged from disclosure or required to be kept confidential by law. In general, an employer may not be held liable on the basis of a communication between a provider and a participant unless the employer knew, or should have known, of the communication before the alleged breach of duty or harm (Idaho Code § 44-202(2)). Participants may not be required to waive the confidential and privileged nature of communications as a condition of participation in the employee assistance

program, but this provision does not apply to an employer's referral of an employee to a provider that is a condition of the employee's continued employment (Idaho Code § 44-202(3)).

Polygraphs: In general, no person, firm, corporation, or other business entity or representative thereof may require, as a condition of employment or continued employment of any person or employee, that the person or employee take a polygraph test. A violation is deemed to be a misdemeanor (Idaho Code § 44-903). However, the prohibition does not apply to any law enforcement agency of the United States, the state of Idaho, or any political subdivision or governmental entity thereof (Idaho Code § 44-904).

Employment of inmates by the state, state agencies, and political subdivisions: Under specific provisions in the Credit Report Protection Act, the state of Idaho, or a department, agency, board, commission, or other political subdivision, may not employ or contract for the employment of an inmate in any facility operated by the Department of Corrections, a private correctional facility, or a county jail in a capacity that would allow an inmate access to any other person's personal information (Idaho Code § 28-52-108(2)).

New hire information: Under laws requiring employers to provide new hire information to the Idaho Department of Labor (Idaho Code § 72-1601 et seq.), any state agency obtaining information collected for these purposes must maintain the confidentiality of the information except as otherwise provided in the law governing the new hire directory. Any employee or agent of the state disclosing information in violation of this requirement commits a misdemeanor (Idaho Code § 72-1605(2)).

Breach notification requirements: Employers who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

7. Insurance –

Regulations governing nonpublic personal information held by insurers: No person required to be licensed or authorized under Idaho insurance law may disclose nonpublic personal information contrary to the provisions of the federal Gramm-Leach-Bliley Act applicable to insurers (Idaho Code § 41-1334(1)). The Insurance Commissioner is authorized by law to promulgate regulations to carry out these provisions (Idaho Code § 41-1334(2)) and has done so at Idaho Regs. § 18.01.48.000 et seq. The law does not create any private cause of action (Idaho Code § 41-1334(3)). The regulations are outlined in detail below.

Scope and primary definitions: The regulations govern the treatment of nonpublic personal financial information about individuals by all licensees of the Idaho Department of Insurance. The rules require licensees to provide notice to individuals about their privacy policies and practices, describe the conditions under which licensees may disclose nonpublic personal information about individuals to affiliates and nonaffiliated third parties, and provide methods to allow individuals to prevent a licensee from disclosing such information (*Idaho Regs. § 18.01.48.001.02*). The rules apply to nonpublic personal financial information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family, or household purposes, but not to information about companies or natural persons who obtain products or services for business, commercial, or agricultural purposes (*Idaho Regs. § 18.01.48.001.03*).

The regulations define "licensees" to include all licensed insurers, producers, and other persons who are licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered under Idaho law (Idaho Regs. § 18.01.48.011.04). Licensees are not subject to the notice and opt-out provisions outlined below if they are employees or agents of another licensee acting as principal, the principal otherwise complies with the requirements, and the licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates (Idaho Regs. § 18.01.48.011.04.a). Licensees also include unlicensed insurers accepting business placed through licensed excess lines brokers under specified conditions (Idaho Regs. § 18.01.48.011.04.b through Idaho Regs. § 18.01.48.011.04.e).

"Nonpublic personal financial information" is personally identifiable financial information and any list, description, or other grouping of consumers derived using any personally identifiable financial information that is not publicly available. The term does not include health information or specified publicly available information (Idaho Regs. § 18.01.48.011.07).

Initial notice: Licensees must provide an initial notice to an individual who becomes the licensee's customer no later than when a customer relationship is established, or to a consumer before the licensee discloses nonpublic personal financial

information to any nonaffiliated third party (Idaho Regs. § 18.01.48.100.01). Initial notice to a consumer is not required if the licensee does not disclose any information about the consumer to a nonaffiliated third party except as allowed by the regulations, or a notice has been provided by an affiliate entity that meets regulatory requirements (Idaho Regs. § 18.01.48.100.02). The law provides specific examples of when a customer relationship is established (Idaho Regs. § 18.01.48.100.03). With respect to existing customers buying new products, a licensee satisfies the initial notice requirement if it provides a revised policy notice or if the initial, revised, or annual notice previously given was accurate with respect to the new product (Idaho Regs. § 18.01.48.100.04). Certain exceptions apply when establishing the customer relationship is not at the customer's election or when notice would substantially delay the transaction (Idaho Regs. § 18.01.48.100.05).

Annual and revised notices: In general, licensees must provide an annual privacy notice to customers (Idaho Regs. § 18.01.48.150.01). Licensees are not required to provide annual notice to former customers (Idaho Regs. § 18.01.48.150.02.a) and do not need to provide an annual privacy notice to a current customer if the licensee provides nonpublic personal financial information to nonaffiliated third parties only in accordance with regulatory requirements and has not changed its policies from those disclosed in the most recent notice sent to consumers (Idaho Regs. § 18.01.48.150.02.b). The law specifies the requirements regarding the contents of privacy notices, including provisions regarding the description of parties subject to exceptions, examples of privacy notice information requirements, requirements for short-form initial notice with opt-out notice for non-customers, information on future disclosures, and sample clauses (Idaho Regs. § 18.01.48.200 through Idaho Regs. § 18.01.48.205 and Idaho Regs. § 18.01.48, Appendix A), as well as requirements for revising privacy notices (Idaho Regs. § 18.01.48.300) and delivery of privacy notices (Idaho Regs. § 18.01.48.350).

Opt-out notices: With respect to opt-out notices, licensees must provide clear and conspicuous notice to consumers that explain the right to opt out. The notice must state that the licensee discloses or reserves the right to disclose nonpublic financial information about a consumer and that the consumer has the right to opt out of the disclosure, together with a reasonable means by which the customer may opt out (Idaho Regs. § 18.01.48.250.01). The regulations provide examples of adequate opt-out notices, and reasonable and unreasonable opt-out means (Idaho Regs. § 18.01.48.250.02 through Idaho Regs. § 18.01.48.250.04.). Licensees may require consumers to opt out through a specific means, so long as the means is reasonable (Idaho Regs. § 18.01.48.250.05).

The opt-out notice may be provided on the same written or electronic form as the initial notice form, but if it is provided subsequent to the initial notice, a copy of the initial notice must accompany the opt-out notice in writing or, if the consumer agrees, electronically (Idaho Regs. § 18.01.48.251.01-02). Specific conditions apply to opt-out requirements regarding consumers in joint relationships (Idaho Regs. § 18.01.48.251.03). Licensees must comply with a consumer opt-out as soon as reasonably practicable after receiving it, and the consumer may exercise the right at any time (Idaho Regs. § 18.01.48.251.04-05). The opt-out is effective until the consumer revokes it. When a customer relationship terminates, the licensee must continue to comply with any opt-out direction in effect at the time of termination, but if a customer relationship is reestablished, the prior opt-out notice does not apply to the new relationship (Idaho Regs. § 18.01.48.251.06).

Limitations on disclosure: A licensee may not disclose nonpublic personal financial information about a consumer to a nonaffiliated third party unless the licensee has provided an initial notice to the consumer and an opt-out notice as provided above, the licensee gives the consumer a reasonable opportunity to opt out prior to disclosing the information, and the consumer does not opt out. The regulation provides examples of actions constituting a reasonable opportunity to opt out (Idaho Regs. § 18.01.48.400.01). Licensees must comply with these requirements with respect to all consumers regardless of whether a consumer has established a customer relationship, and unless a licensee complies with regulatory requirements, it may not disclose any nonpublic personal financial information about an individual that it has collected, regardless of whether the licensee collected it before or after receiving a direction to opt out from the consumer (Idaho Regs. § 18.01.48.400.02). Consumers may select the portions of their nonpublic personal financial information or certain nonaffiliated third parties with respect to which they choose to exercise the opt-out (Idaho Regs. § 18.01.48.400.03).

Licensees that receive nonpublic personal financial information from a nonaffiliated financial institution under a regulatory exception (see below) may only disclose the information to the affiliates of the financial institution from which it received the information, to its affiliates, or in the ordinary course of business to carry out the activity giving rise to the exception. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention or in response to a properly authorized subpoena. The licensee may not disclose such information to a third party for marketing purposes or use the information for its own marketing purposes

(Idaho Regs. § 18.01.48.401.01). Similar restrictions to those outlined above apply to information received from a nonaffiliated financial institution outside an exception (Idaho Regs. § 18.01.48.401.02). If a licensee discloses information to a nonaffiliated third party under a regulatory exception, the third party may only disclose the information to the licensee's affiliates, to its own affiliates, or in the ordinary course of business to carry out the activity giving rise to the exception. Similar requirements apply to information disclosed to a nonaffiliated third party outside an exception (Idaho Regs. § 18.01.48.401.03-04).

Licensees also are prohibited from disclosing policy numbers or similar access numbers or codes to any nonaffiliated third party for marketing purposes, unless a statutory exception applies (Idaho Regs. § 18.01.48.402).

Exceptions to notice or opt-out requirements: The opt-out requirements described above do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party performing a service for the licensee if the licensee provides the initial notice described above and enters into a contractual agreement with the third party prohibiting it from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information (Idaho Regs. § 18.01.48.450.01). The services a nonaffiliated third party performs for a licensee as outlined above may include marketing of the licensee's own products or services offered pursuant to a written agreement between the licensee and one or more financial institutions to jointly offer, endorse, or sponsor a financial product or service (Idaho Regs. § 18.01.48.450.02).

Initial notice and opt-out requirements, including those related to joint marketing activities, do not apply if the licensee discloses nonpublic personal financial information that is necessary to effect, administer, or enforce a transaction requested by the consumer in connection with specified purposes. The regulation provides examples of activities deemed necessary to effect, administer, or enforce a transaction (Idaho Regs. § 18.01.48.451). Other exceptions apply to licensee disclosures where the consumer has consented to the disclosure, disclosures to protect the confidentiality or security of a licensee's records or protect against actual or potential fraud, disclosures to provide information to insurance rate advisory organizations or other regulators, or specified disclosures authorized under federal law, among others (Idaho Regs. § 18.01.48.452.01). A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures as outlined above (Idaho Regs. § 18.01.48.452.02).

FCRA and nondiscrimination requirements: The regulations do not modify, limit, or supersede the operations of the federal Fair Credit Reporting Act (FCRA), and no inference may be drawn on the basis of the regulations as to whether information is transaction or experience information under that law (Idaho Regs. § 18.01.48.500). Licensees may not discriminate against any consumer or customer who opts out from disclosure of nonpublic personal financial information (Idaho Regs. § 18.01.48.501).

Violations: Any person who releases nonpublic personal information in violation of the regulations or otherwise fails to comply with the rules may be found by the Director of Insurance to be in violation of the trade practices and frauds chapter of Idaho insurance law and subject to the penalties in that law (Idaho Regs. § 18.01.48.502; see Section II.C. and Section I.H.).

Prohibition on release of patient-identifying prescription information: No person may release or sell, or include in any policy of insurance delivered or issued for delivery in Idaho any provision for the release or sale of, any information related to prescriptions, drug orders, records, or other prescription information that specifically identifies an insured individual, except as provided in Idaho Code § 54-1727 regarding permissible releases of such information by pharmacists (see Section I.D.9.) (Idaho Code § 41-1335(1)). In addition to any other penalties prescribed by law, a violator is subject to an administrative penalty not to exceed $3,000 (Idaho Code § 41-1335(2)). A person who releases information in good faith pursuant to Idaho Code § 54-1727 is not subject to penalty, liability, or a cause of action for any loss or damage based on the release of such records or information (Idaho Code § 41-1335(3)).

Breach notification requirements: Insurers who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

8. Retail & Consumer Products –

Breach notification requirements: Persons engaged in the retail and consumer products sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

9. Social Media –

Breach notification requirements: Persons engaged in the social media sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

10. Tech & Telecom –

Breach notification requirements: Persons engaged in the tech and telecommunications sector who own or license computerized data including personal information are subject to breach notification requirements (see Section I.C.8.).

Anti-spam law: For information on provisions of the state's anti-spam law applicable to interactive service providers, see Section I.E.1.

Electronic surveillance: For information on provisions applicable to telecommunications providers with respect to the interception of communications, see Section I.F.

11. Other Sectors –

Our research has revealed no specific Idaho law provisions applicable to other business sectors.

F. Electronic Surveillance –

In general: A person is guilty of a felony punishable by up to five years in prison or a fine of not more than $5,000, or both, if the person does any of the following:

- willfully intercepts, endeavors to intercept, or procures another to intercept or endeavor to intercept a wire, oral, or electronic communication; or
- willfully uses, endeavors to use, or procures another to use any electronic, mechanical, or other device to intercept an oral communication when the device is affixed to or otherwise transmits a signal through a wire, cable, or other connection or transmits communications by radio or interferes with the transmission;
- willfully discloses, or endeavors to disclose, to any other person the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained in violation;
- willfully uses, or endeavors to use, the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained in violation; or
- intentionally discloses or endeavors to disclose to any other person the contents of any wire, oral, or electronic communication intercepted in connection with specified activities involving criminal investigations if the person knows or has reason to know that the information was obtained in connection with a criminal investigation and the person has obtained the information in an attempt to obstruct, impede, or interfere with such investigation (Idaho Code § 18-6702(1)).

It is lawful for an operator of a switchboard, or for an officer, employee, or agent of any wire or electronic communication provider whose facilities are used in the transmission of a wire communication to intercept, disclose, or use the communication or the identity of any party to the communication in the normal course of employment while engaged in any activity necessarily incident to the rendition of his service or to the protection of the rights or property of the carrier or provider of communications services. Providers may not utilize service observing or random monitoring except for mechanical, service quality, or performance control checks (Idaho Code § 18-6702(2)(a)). It also is lawful for an officer, employee, or agent of the FCC, in the normal course of employment, and in the discharge of specified monitoring responsibilities under federal law, to intercept a wire, oral, or electronic communication transmitted by radio or to disclose or use the information obtained from the interception (Idaho Code § 18-6702(2)(b)).

It is lawful for a law enforcement officer or person acting under color of law to intercept a wire, oral, or electronic communication when such person is a party to the conversation or one of the parties to the communication has given prior consent (Idaho Code § 18-6702(2)(c)). In addition, it is lawful for a person to intercept a wire, oral, or electronic communication when such person is a party to the conversation or one of the parties to the communication has given prior

consent (Idaho Code § 18-6702(2)(d)). Accordingly, Idaho is a "one-party consent" state. It is unlawful to intercept any communication for purpose of committing any criminal act (Idaho Code § 18-6702(2)(e)).

It is lawful for an employee of a telephone company to intercept a wire communication for the sole purpose of tracking the origin of the communication when requested by an appropriate law enforcement agency or when requested by a recipient of a communication that the recipient alleges is obscene, harassing, or threatening (Idaho Code § 18-6702(2)(f)). It is also lawful for employees of law enforcement agencies, fire departments, or ambulance services, while acting in the scope of their employment, to intercept and record incoming wire or electronic communications (Idaho Code § 18-6702(2)(g). Finally, additional exceptions are provided for interceptions made via communication systems readily available to the public; public radio transmissions or transmissions related to ships, aircraft, civil defense systems, citizen's band radio frequencies, or marine or aeronautical communications systems; interceptions of transmission causing harmful interference; or interceptions by users of the same frequency where the transmission is not scrambled or encrypted (Idaho Code § 18-6702(h)). Providers of electronic communications service may record the fact that a wire or electronic communication was initiated or completed to protect itself, another provider, or user of the service from fraudulent, unlawful, or abusive use of the service (Idaho Code § 18-6702(2)(i)).

Persons or entities providing electronic communications services to the public generally may not intentionally divulge the contents of any communication other than to such person or entity while in transmission on that service, to any person or entity other than an addressee or intended addressee of the communication (Idaho Code § 18-6702(3)(a)). Such communications may be divulged by the electronic communications provider under specified circumstances, including as otherwise authorized above; with the lawful consent of the originator or any addressee or intended addressee; to a person employed or authorized, or whose facilities are used, to forward such communications; or if the contents were inadvertently obtained by the provider and appear to pertain to the commission of a crime, in which case the provider may divulge them to a law enforcement agency (Idaho Code § 18-6702(3)(b)).

Any person whose wire, oral, or electronic communication is intercepted, used, or disclosed in violation of the requirements outlined above may bring a civil cause of action against the violator (Idaho Code § 18-6709; see Section I.G.5.).

Drones: In general, absent a warrant or for emergency response for search and rescue or a controlled substance investigation, no person, entity, or state agency may use an unmanned aircraft system to intentionally conduct surveillance on specifically targeted persons or private property or use such a drone to photograph or record an individual for purposes of publishing or disseminating the photograph or recording without the individual's written consent (Idaho Code § 21-213(2)). A person subject to such prohibited conduct has a civil cause of action against the violator (Idaho Code § 21-213(3); see Section I.G.5.). Owners of facilities located on land owned by another under a valid easement, permit, or other right of occupancy may use drones to aerially inspect such facilities (Idaho Code § 21-213(4)).

G. Private Causes of Action

1. Consumer Protection –

Limitations on information on payment card receipts: Merchants violating provisions prohibiting the printing of more than the last five digits of a payment card account number or the card's expiration date (see Section I.D.3.) are subject to a civil penalty of not more than $250 for a first violation and $1,000 for second and subsequent violations. An action to recover the penalty may be brought by a prosecuting attorney, but if the prosecuting attorney does not bring such an action within 60 days of the date the violation is reported by the cardholder, the cardholder may bring the action. The penalties above are in addition to any remedies available to the cardholder. The penalty is paid into the state's general fund, not to the cardholder, but attorney fees are available to the party successfully bringing the action (Idaho Code § 28-51-103(3)).

Security freezes: A consumer reporting agency (CRA) that willfully fails to comply with any requirement imposed by the security freeze law with respect to any consumer (see Section I.D.4.) is liable to the consumer for the sum of any actual damages or damages of not less than $100 nor more than $1,000; punitive damages as allowed by the court; and in the case of a successful action, the costs of the action and reasonable attorney fees (Idaho Code § 28-52-109(1)). Any person who obtains a consumer report, requests a security freeze, requests a temporary lifting of a freeze, or requests a removal of a freeze from a CRA under false pretenses or in an attempt to violate state or federal law is liable to the CRA for actual

damages or $1,000, whichever is greater (Idaho Code § 28-52-109(2)). A CRA that is negligent in failing to comply with the security freeze requirements is liable to the consumer in an amount equal to any actual damages and, in the case of a successful action, costs of the action and reasonable attorney fees (Idaho Code § 28-52-109(3)). [Note: The Attorney General has exclusive jurisdiction to bring an action against a consumer reporting agency (CRA) with respect to violations involving the failure of a CRA to temporarily lift a security freeze within 15 minutes. For information concerning the remedies available in such an action, see Section II.C.].

If the court finds that any pleading, motion, or other paper filed in connection with an action as outlined above was filed in bad faith or for purposes of harassment, the court must award attorney fees to the prevailing party reasonable in relation to the work expended in responding (Idaho Code § 28-52-109(4)).

Anti-spam law: Recipients of bulk e-mail advertisements sent in violation of the state's anti-spam law (see Section I.E.1.) are entitled to bring a cause of action to recover actual damages under Idaho Code § 48-608 governing damages available for unlawful methods or practices under the state's consumer protection law. Under this law, such damages include actual damages or $1,000, whichever is greater. In lieu of actual damages, a recipient may elect to recover the greater of $100 for each bulk e-mail advertisement transmitted to the recipient in violation of the law, or $1,000 (Idaho Code § 48-603E(4)). It should be noted, however, that the federal CAN-SPAM Act preempts state claims that are not based on traditional tort theories of falsity and deception (15 U.S.C. § 7707(b)(1)).

2. Identity Theft –

Idaho law specifies several offenses constituting identity theft, as outlined in detail below. For purposes of these crimes, "personal identifying information" is defined as the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, checking account number, savings account number, financial transaction card number, or personal identification code of an individual person, or any other numbers or information that can be used to access a person's financial resources (Idaho Code § 18-3122(10)).

Misappropriation of personal identifying information: It is unlawful for any person to obtain or record personal identifying information of another person, without that person's authorization, with the intent that the information be used to obtain or attempt to obtain credit, money, goods, or services without the consent of that person (Idaho Code § 18-3126). The crime is a felony (Idaho Code § 18-3128(1)), punishable by a fine of up to $50,000 or imprisonment for up to five years, or both (Idaho Code § 18-3128(3)).

Acquisition of personal identifying information by false authority: It is unlawful for any person to falsely assume or pretend to be a member of the armed forces of the United States or an officer or employee acting under the authority of the United States or any department, agency, or office thereof, or of the state of Idaho or any department, agency, or office thereof, and as such a pretended character, seek, demand, obtain, or attempt to obtain personal identifying information about another person (Idaho Code § 18-3126A). The crime is a felony (Idaho Code § 18-3128(1)), punishable by a fine of up to $50,000 or imprisonment for up to five years, or both (Idaho Code § 18-3128(3)).

Receiving or possessing fraudulently obtained goods or services: It is unlawful for any person to receive, retain, conceal, possess, or dispose of personal property, cash, or another thing of value when the person knows that the item of value has been obtained through fraudulent means, including misappropriation of personal identifying information (Idaho Code § 18-3127). A violation of this provision is a misdemeanor, unless the retail value of the goods at issue exceeds $300, in which case the crime is a felony (Idaho Code § 18-3128(1)). A misdemeanor is punishable by a fine of up to $1,000 or imprisonment of up to one year, or both (Idaho Code § 18-3128(2)). A felony is punishable by a fine of up to $50,000 or imprisonment for up to five years, or both (Idaho Code § 18-3128(3)).

3. Invasion of Privacy –

Invasion of privacy claims in Idaho generally are covered by common law doctrine. The state's law prohibiting video voyeurism (Idaho Code § 18-6609) is outlined at Section I.H. In addition, a number of sector-specific laws contain provisions related to what would generally be considered an invasion of privacy, including prohibitions on electronic surveillance (see Section I.F.), among others.

4. Computer Hacking –

A person who does any of the following commits a computer crime under Idaho law:

- knowingly accesses, attempts to access, uses, or attempts to use any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud, obtaining money, property, or services by means of false or fraudulent pretenses, or committing theft (Idaho Code § 18-2202(1));
- knowingly and without authorization alters, damages, or destroys any computer, system, or network, or any computer software, program, documentation, or data contained therein (Idaho Code § 18-2202(2)); or
- knowingly and without authorization uses, accesses, or attempts to access any computer, system or network, or any computer software, program, documentation, or data contained therein (Idaho Code § 18-2202(3)).

The first two crimes outlined above are classified as felonies, while the third is classified as a misdemeanor (Idaho Code § 18-2202(4)).

5. Other Causes of Action –

Access to records under Public Records Act: A person aggrieved by the denial of a request for disclosure of information contained in records subject to the Public Records Act (see Section I.C.10.) may bring an action in district court within 180 days from the date of mailing of the notice of denial. The law sets forth the procedural requirements regarding such an action (Idaho Code § 74-115). The court may order a public official to disclose a public record or show cause why it should not do so. If the court finds that an official's decision not to disclose is not justified, it must order the disclosure, and if it finds that the decision was justified, it must return the item to the official without making a disclosure. In either case, the court must award reasonable attorney fees and costs to the prevailing party, if it finds that the request or refusal to provide records was frivolously pursued (Idaho Code § 74-116; see also Idaho Code § 74-113(2)). Finally, if the court finds that a public official has deliberately and in bad faith improperly refused a legitimate request for inspection and copying, a civil penalty must be assessed against the official not to exceed $1,000 (Idaho Code § 74-117).

Electronic surveillance: Any person whose wire, oral, or electronic communication is intercepted, used, or disclosed in violation of requirements governing electronic surveillance in Idaho (see Section I.F.) may bring a civil cause of action against the violator. Such person may recover actual damages, but not less than liquidated damages of $100 per day for each day of violation or $1,000, whichever is higher, plus punitive damages and reasonable attorney fees and other litigation costs. Good faith reliance on a court order constitutes a complete defense to any civil or criminal action (Idaho Code § 18-6709).

Drones: A person subject to illegal surveillance through the use of an unmanned aircraft system, or drone, has a civil cause of action against the violator and is entitled to recover damages of the greater of $1,000 or actual and general damages, plus reasonable attorney fees and other litigation costs (Idaho Code § 21-213(3).

H. Criminal Liability –

Criminal penalties applicable to governmental employees: Under the state's data breach notification law (see Section I.C.8.), any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor punishable by a fine of not more than $2,000, imprisonment for up to one year, or both (Idaho Code § 28-51-105(1), third paragraph).

Criminal history record information: It is a misdemeanor for a person, for personal gain, to request, obtain, or attempt to obtain criminal history records under false pretenses or willfully communicate or attempt to communicate criminal history records to any agency or person not authorized to receive the information (Idaho Code § 67-3009(1)). In addition, it is unlawful to willfully solicit, accept, or agree to accept from another any pecuniary benefit as consideration either for willfully falsifying criminal history records or willfully requesting, obtaining, or seeking to obtain such records for an unauthorized purpose. A violation of this provision is a felony subject to a fine of up to $10,000 and imprisonment for up to five years

(Idaho Code § 67-3009(2)). For more information on requirements relating to access to, and correction and disclosure of, criminal history record information, see Section I.D.5.

HIV/AIDS and other venereal diseases: Any person who willfully or maliciously discloses information related to HIV/AIDS and other venereal diseases (see Section I.D.9.) to any third party, except pursuant to written authorization by the data subject, is guilty of a misdemeanor (Idaho Code § 39-606).

Polygraphs: In general, no person, firm, corporation, or other business entity or representative thereof may require, as a condition of employment or continued employment of any person or employee, that the person or employee take a polygraph test (see Section I.E.6.). A violation is deemed to be a misdemeanor (Idaho Code § 44-903).

Regulations governing nonpublic personal information held by insurers: Any person who releases nonpublic personal information in violation of the regulations governing the collection, use, and disclosure of nonpublic personal financial information applicable to insurers (see Section I.E.7.) or otherwise fails to comply with the rules may be found by the Director of Insurance to be in violation of the trade practices and frauds chapter of Idaho insurance law and subject to the penalties in that law (Idaho Regs. § 18.01.48.502). Under that law, in addition to prescribed administrative penalties (see Section I.C.), on a criminal conviction, a person is subject to a fine of not more than $1,000 or imprisonment not to exceed six months, or both. Each instance of violation is considered a separate offense (Idaho Code § 41-117).

Video voyeurism and revenge porn: A person is guilty of video voyeurism when, with intent to arouse, appeal to, or gratify the passions or sexual desires of the person or another, or for his own lascivious entertainment or satisfaction or prurient interest, or for the purpose of sexually degrading or abusing any person, the person uses, installs, or permits the use or installation of an imaging device in a place where a person would have a reasonable expectation of privacy, without the consent or knowledge of the person using the place (Idaho Code § 18-6609(2)).

With respect to activity commonly referred to as "revenge porn," the law provides that a person commits video voyeurism when, with intent to annoy, terrify, threaten, intimidate, harass, offend, humiliate, or degrade, the person intentionally disseminates, publishes, or sells, or conspires to disseminate, publish, or sell, any image of another person who is identifiable from the image itself or information displayed in connection with the image and whose intimate areas are exposed or who is engaged in a sexual act, provided the person knew or reasonably should have known that the person depicted understood that the image was to remain private and that the person depicted did not consent to the dissemination, publication, or sale (Idaho Code § 18-6609(3)).

A violation is characterized as a felony (Idaho Code § 18-6609(4)). Interactive computer services, information services, and telecommunications services are not liable for content provided by another person unless the service intentionally aids or abets the crime (Idaho Code § 18-6609(5)(a). The law does not apply to images involving voluntary exposure in public or commercial settings, or to disclosures made in the public interest, including reporting of unlawful conduct or the lawful and common practices of law enforcement, criminal reporting, legal proceedings, or medical treatment (Idaho Code § 18-6606(5)(b)-(c)).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. Attorney General –

The Attorney General is responsible for the enforcement of most privacy and data protection laws in Idaho, including the state's data breach provisions (see Section I.C.8.) and security freeze provisions (see Section I.D.4.).

B. Other Regulators –

The State Board of Education is responsible for implementing the provisions of the Student Data Accessibility, Transparency and Accountability Act (SDATAA) (see Section I.E.2.).

The Department of Insurance enforces regulations under its jurisdiction regarding the privacy of nonpublic personal financial information of consumers and customers of insurers regulated under Idaho law (see Section I.E.7.).

C. Sanctions & Fines –

Data breach notification law: For purposes of the state's data breach notification law (see Section I.C.8.), if the primary regulator of an agency, individual, or commercial entity has reason to believe that the agency, individual, or entity has violated the notification requirements, the primary regulator may bring a civil action to enforce compliance and to enjoin the agency, individual, or entity from further violations. An agency, individual, or commercial entity that intentionally fails to give notice in accordance with the law is subject to a fine of not more than $25,000 per breach of the security of the system (Idaho Code § 28-51-107).

Limitations on information on payment card receipts: Merchants violating provisions prohibiting the printing of more than the last five digits of a payment card account number or the card's expiration date (see Section I.D.3.) are subject to a civil penalty of not more than $250 for a first violation and $1,000 for second and subsequent violations. An action to recover the penalty may be brought by a prosecuting attorney, but if the prosecuting attorney does not bring such an action within 60 days of the date the violation is reported by the cardholder, the cardholder may bring the action. The penalties above are in addition to any remedies available to the cardholder. The penalty is paid into the state's general fund, not to the cardholder, but attorney fees are available to the party successfully bringing the action (Idaho Code § 28-51-103(3)).

Security freeze law: The Attorney General may enforce the provisions of the security freeze law (see Section I.D.4.). In addition, the Attorney General has exclusive jurisdiction to bring an action against a consumer reporting agency (CRA) with respect to violations involving the failure of a CRA to temporarily lift a security freeze within 15 minutes. In any such action, a CRA in violation is subject to a civil penalty of not less than $100 nor more than $1,000 for a violation or series of violations concerning a specific consumer and no greater than $100,000 in the aggregate for related violations concerning more than one consumer. The Attorney General also may seek injunctive relief to prevent future violations (Idaho Code § 28-52-109(5)).

Physicians: Physicians, physician assistants, interns, and residents are subject to discipline by the Board of Medicine for failure to safeguard the confidentiality of medical records or other information pertaining to identifiable patients (Idaho Code § 54-1814(13)). In any such disciplinary action, the Board may, among other penalties, suspend, limit, or revoke a physician's license and may impose an administrative penalty of up to $10,000 (Idaho Code § 54-1806A(9)).

Pharmacists: Persons found to be in violation of requirements related to the confidentiality of prescription, drug record, and related information held by pharmacists (see Section I.D.9.) are subject to an administrative penalty of not more than $3,000 per violation (Idaho Code § 54-1727(5)). However, no person is liable for any loss or damage based on a good faith release of records (Idaho Code § 54-1727(6)).

Chiropractors: The State Board of Chiropractic Physicians may restrict, suspend, or revoke the license of a chiropractor who fails to safeguard the confidentiality of chiropractic records or other information pertaining to an identifiable client (Idaho Code § 54-712(7)). The law provides for the imposition of such discipline (Idaho Code § 54-713) and specifies that a chiropractor found in violation may be subject to an administrative fine of up to $2,000 (Idaho Code § 54-713(1)(f)).

Cancer registry: No action may be brought against reporting entities or their employees who participate in the cancer registry program (see Section I.D.9.) in good faith (Idaho Code § 57-1707(1)). In addition, the license of a facility or health care provider may not be denied, suspended, or revoked for the good faith disclosure of confidential or privileged information in accordance with program requirements (Idaho Code § 57-1707(2)). However, such immunity does not apply to disclosures made due to gross negligence or willful misconduct of the reporting entity (Idaho Code § 57-1707(3)).

SDATAA : Under the Student Data Accessibility, Transparency and Accountability Act (SDATAA; see Section I.E.2.), the Board of Education has developed a model policy for school districts and public charter schools that governs data collection, access, security, and use, and each school district and charter school must adopt the policy. Any district or public charter school that fails to adopt the policy where any inappropriate release of data occurs is liable for a civil penalty of up to $50,000 per violation, recoverable in a civil action by the Board, with the assistance of the Attorney General (Idaho Code § 33-133(7)).

Regulations governing nonpublic personal information held by insurers: Any person who releases nonpublic personal information in violation of the regulations governing the collection, use, and disclosure of nonpublic personal financial information applicable to insurers (see Section I.E.7.) or otherwise fails to comply with the rules may be found by the Director of Insurance to be in violation of the trade practices and frauds chapter of Idaho insurance law and subject to the penalties in that law (Idaho Regs. § 18.01.48.502). Under that law, in addition to prescribed criminal penalties (see Section I.H.), a person in violation, or who violates a cease-and-desist order issued by the Director, is subject to the general penalty prescribed under the insurance law (Idaho Code § 41-1327). This penalty, in addition to any applicable denial, suspension, or revocation of a certificate of authority or license, is not more than $1,000 for any individual or natural person and not more than $5,000 for any other person (Idaho Code § 41-117).

Prohibition on release of patient-identifying prescription information: A person who releases or sells, or includes in any policy of insurance delivered or issued for delivery in Idaho any provision for the release or sale of, any information related to prescriptions, drug orders, records, or other prescription information that specifically identifies an insured individual in violation of provisions of insurance law prohibiting such sale or release (see Section I.E.7.) is, in addition to any other penalties prescribed by law, subject to an administrative penalty not to exceed $3,000 (Idaho Code § 41-1335(2)). A person who releases information in good faith pursuant to Idaho Code § 54-1727 governing permissible releases of such information by pharmacists is not subject to penalty, liability, or a cause of action for any loss or damage based on the release of such records or information (Idaho Code § 41-1335(3)).

D. Representative Enforcement Actions –

Our research has uncovered no published enforcement actions regarding privacy and data security by Idaho state agencies.

E. State Resources –

The Attorney General has provided guidance for consumers on registering with the National Do-Not-Call Registry, as well as a variety of manuals designed to address consumer protection issues.

The Idaho Transportation Department has developed a Guide to Understanding Driving Records.

The State Board of Education has drafted a model student data privacy and security policy for use by school districts and public charter schools in implementing measures regarding the collection, access, security, and use of student data.

III. RISK ENVIRONMENT –

Idaho has a history of following convention when it comes to data privacy and security legislation. Idaho's data breach notification law was adopted in 2006 after nearly half of U.S. states had already adopted such legislation. The Idaho data breach notification law is modeled after Delaware's law, which according to the law's sponsor has "a simple process that is not vindictive" toward business (Comments of Representative Max Black before the House State Affairs Committee on March 13, 2006). Violators of the Idaho data breach notification law are subject to a fine, not to exceed $25,000 per data breach, for failing to notify Idaho residents of a breach, as required by the law (Idaho Code Section 28-51-107). The Idaho Legislature amended the state's data breach notification law in 2010 to apply to city, county, and state agencies in response to an incident in which the Idaho Soil Conservation Commission's website was shut down within 24 hours after the Attorney General's Office was contacted about the Commission regularly posting personal information from their minutes on its website.

After more than three-quarters of U.S. states passed consumer reporting laws complementary of the federal Fair Credit Reporting Act (15 U.S.C. § 1681), Idaho adopted the Credit Report Protection Act in 2008, which expands Idaho consumers' rights in connection with their credit information (Idaho Code § 28-52-101). A year after Equifax's data breach that exposed the personal data of a majority of American adults, the Idaho Legislature in 2018 amended the Credit Report Protection Act to further restrict the fees charged by consumer credit reporting agencies for placement of credit report security freezes.

The Idaho Legislature did not consider any significant data privacy or security legislation in 2019 and there is no indication Idaho will be an early adopter of the privacy rights recognized by the California Consumer Protection Act or the European Union's General Data Protection Regulation.

A. Attorney General Enforcement

For more than a decade, Attorney General Lawrence Wasden has participated in privacy and security enforcement investigations with other U.S. states, resulting in settlement payments and agreements that require the businesses to change their privacy practices and data security measures. As of September 2019, Attorney General Wasden has announced three notable settlements with businesses in 2019 and confirmed Idaho's participation in the Google and Facebook investigations. In July 2019, Attorney General Wasden joined all of the other state Attorneys General in a settlement with Equifax that involved a $175 million payment to the states and a $300 million payment to a Consumer Restitution Fund for the benefit of affected consumers, with the possibility of paying up to an additional $125 million into the settlement fund, for a total of $425 million. Attorney General Wasden also announced in July 2019 that Idaho was one of 30 states settling with Premera Blue Cross following a breach that exposed personal information of more than 270,000 Idahoans and 10.4 million people throughout the U.S. Along with 42 other states and the District of Columbia, Idaho reached a settlement with the Neiman Marcus Group LLC in January 2019. These 2019 enforcement actions have contributed more than $1.3 million to Idaho's Consumer Protection Fund. Attorney General Wasden's data privacy approach extends beyond enforcement actions, with a particular emphasis on educating Idaho consumers about scams and Internet safety interests. The Idaho Attorney General's Office often makes public announcements and engages in other communications with Idaho consumers regarding security incidents and scams that may expose them to possible identity theft or other types of fraud. The Office has also published manuals on Identify Theft, Internet Safety, and Consumer Protection, which contains a number of sections on privacy, data security, and credit reporting.

Attorney General Wasden has encouraged businesses to provide consumers with the ability to make choices about data posted by them, saying in a 2014 interview with the International Association of Privacy Professionals (IAPP): "I think that one of the best steps that a social media or networking business can take is to be proactive in allowing teens and their parents the ability to remove and shut down posts and information. In other words, take steps that make [California's 'Eraser Button'] legislation unnecessary." In the same interview, Attorney General Wasden said that when legislation is necessary, he thinks it is important for "businesses [to] interact early and often with those introducing the legislation to ensure what is proposed reflects achievable improvements and remedies for businesses and constituents" (IAPP interview by Divonne Smoyer and Frederick Lah with Lawrence Wasden, Attorney General, Idaho Attorney General's Office (October 28, 2014)).

Attorney General Wasden is Idaho's longest-serving Attorney General. He has served as president of the National Association of Attorneys General and the chair of the Conference of Western Attorneys General during his lengthy tenure following his 2002 election. Attorney General Wasden was among the 43 Attorneys General who submitted comments in June 2019 to the Federal Trade Commission (FTC) urging the FTC to increase antitrust enforcement in technology platform mergers and acquisitions and further consider privacy protection and consumer choice among the non-price effects in the FTC's merger analysis.

B. Court Actions and State Enforcement

As of September 2019, there are no published decisions by Idaho courts or state agencies regarding data privacy or security. This section will be updated to reflect new developments.

IV. EMERGING ISSUES AND OUTLOOK

A. Recent Legislation

1. Revenge porn –

HB 584, enacted Mar. 26, 2018, and effective Jul. 1, 2018, modified several definitions related to the crime of video voyeurism and amended the law to provide further specification with respect to offenses that constitute what is commonly referred to as revenge porn (see Section I.H.).

2. Security freeze fees –

SB 1265, enacted Mar. 20, 2018, and effective Jul. 1, 2018, allows Idaho residents to place one security freeze on a credit report and one temporary lift of such a freeze every 12 months at no cost to the consumer (see Section I.D.4.).

3. Personnel records of public officials and employees –

SB 1274, enacted Mar. 19, 2018, and effective Jul. 1, 2018, added social security numbers and driver's license numbers to the categories of personal information not disclosable under the Public Records Act (see Section I.C.10.).

B. Current Session Legislation (2019-2020) –

Click here to view recent state specific privacy and data security legislation. This search is automatically updated to display active bills as they move through the legislative process.

C. Other Issues

1. Equifax Breach –

On July 22, 2019, the Federal Trade Commission (FTC) announced that Equifax will pay at least $575 million and up to $700 million as part of a settlement with the FTC, the Consumer Financial Protection Bureau (CFPB) and 48 states, plus the District of Columbia and Puerto Rico. The settlement resolves allegations that the company failed to adequately protect consumers' data, which ultimately led to the 2017 data breach affecting at least 147 million consumers.

Under the settlement agreement, Equifax will contribute $300 million to a fund created to provide credit monitoring for all consumers affected by the breach and provide an additional $125 million to the fund if the initial amount is insufficient to compensate affected consumers. The fund will also be used to compensate and reimburse consumers who bought credit monitoring services from Equifax and paid other out-of-pocket expenses resulting from the breach. Affected individuals are eligible to receive up to $20,000 for verifiable unreimbursed costs related to the breach. Further, the company will pay $175 million to the 48 states, District of Columbia, and Puerto Rico. CFPB will collect another $100 million in civil penalties. Beginning in 2020, Equifax will provide to all U.S. consumers six free credit reports per year for seven years – in addition to the one free report provided annually by Equifax and two national credit monitoring agencies, TransUnion and Experian.

The FTC's complaint against Equifax alleged that after being alerted in March 2017 to a critical security vulnerability in its consumer inquiry database, the company's security team ordered the system to be patched within 48 hours. However, Equifax failed to ensure the order was executed and learned in July 2017 that the database was unpatched. As a result, for several months, hackers gained access to, and stole, consumers' personally identifiable information, including Social Security numbers, birth dates, credit card numbers, and other sensitive data.

The FTC alleged that Equifax failed to implement basic security measures, such as implementing a policy to ensure security vulnerabilities were patched, failing to install intrusion detection for legacy databases, and failing to encrypt Social Security numbers and other sensitive consumer data. Although the basic security measures were not taken, Equifax's privacy policy stated that it implemented reasonable safeguards to limit access to and protect consumer information. As such, the FTC's complaint alleged that Equifax violated the Gramm-Leach-Bliley Act's Safeguards Rule because "it did not design and implement safeguards to address foreseeable internal and external risks, regularly test or monitor the effectiveness of the safeguards, or evaluate and adjust the information security program in light of the results of testing and monitoring…." Additionally, the FTC alleged that Equifax's failure violated the FTC Act.

In addition to civil penalties and the monetary compensation to affected individuals, Equifax must also create and implement a comprehensive information security program, with a third-party assessment every two years.

2. Facebook/Cambridge Analytica –

In March 2018, Idaho Attorney General Lawrence Wasden 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.

3. Facebook-FTC Settlement –

On July 24, 2019, the Federal Trade Commission (FTC) announced that Facebook will pay $5 billion and implement new privacy restrictions as part of a 20-year settlement agreement for alleged privacy violations. The settlement resolves the FTC's allegations that the company violated a 2012 FTC order and deceived Facebook users about their ability to control the privacy of their personal information. According to the FTC, the monetary fine "is one of the largest penalties ever assessed by the U.S. government for any violation," and is "almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide." The FTC's 2012 order required Facebook to, among other things, give consumers clear notice and obtain express consent before sharing consumers' information, execute and maintain a privacy program to protect consumers' information, and obtain independent third-party privacy audits every other year. However, the FTC alleged in its 2019 complaint that Facebook violated the order because the company did not maintain a privacy program that protected the privacy of consumer's information, it used deceptive privacy settings and statements that users relied on to restrict sharing their information on Facebook, and it shared data of users' Facebook friends with third-party app developers regardless of the friends' privacy settings. Further, Facebook violated Section 5(a) of the FTC Act by failing to disclose that certain user information would be used for advertising. In addition to the $5 billion penalty, Facebook must create an independent privacy committee consisting of Facebook's board of directors, appointed by an independent nominating committee. Facebook must also designate compliance officers to be in charge of the company's new privacy program. The compliance officers, along with CEO Mark Zuckerberg, must submit quarterly and annual compliance certifications to the FTC stating the company is in compliance with the 2019 order. Among other requirements, the company must also implement broader oversight of third-party apps, provide users with clear notice that it uses facial recognition technology, and conduct a privacy review of all new or modified products, services, or practices before implementation.