Bloomberg Law
Privacy & Data Security

Domestic Privacy Profile: PENNSYLVANIA

Abraham J. Rein, of Post & Schell, P.C., Philadelphia, provided expert review of the Pennsylvania Profile and wrote the Risk Environment section. [Last updated January 2018. — Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

There are no provisions in the Pennsylvania Constitution specifically providing a right to privacy. The Pennsylvania Supreme Court, however, has indicated that certain types of personal information implicate a right to informational privacy in art. I, § 1 of the Constitution unless the right is outweighed by a public interest favoring disclosure. *Pennsylvania State Educ. Ass'n v. Commonwealth*, 148 A.3d 142 (Pa. 2016), held that public school employees have a constitutional right to privacy in their home addresses in connection with requests for information under Pennsylvania Right to Know Law, 65 Pa. Stat. § 67.101 *et seq.* It should be noted that the case appears to be limited to information sought under the Right to Know Law, which is applicable only in the context of requests for public records of governmental bodies. In another example, *In re June 1979 Allegheny Cty. Investigating Grand Jury*, 415 A.2d 73, 78 (Pa. 1980) held that under certain circumstances the privacy of confidences revealed by a patient to a physician may be constitutionally protected. See also *In re "B,"* 394 A.2d 419 (Pa. 1989) (plurality opinion); *Commonwealth ex rel. Gorto v. Gorto*, 444 A.2d 1299 (Pa. Super. 1982).

B. PERSONAL DATA PROTECTION PROVISIONS

The primary provision of Pennsylvania privacy laws applicable to private sector businesses and state agencies is the Breach of Personal Information Notification Act (BPINA), 73 Pa. Stat. § 2301 *et seq.*), which is outlined below and discussed in detail at Section I.C.8. There are additional privacy laws, including the chapter on privacy of social security numbers (74 Pa. Stat. § 201 *et seq.*; see Section I.D.10.), the Inspection of Employee Records Law (Personnel Files Act) (43 Pa. Stat. § 1321 *et seq.*; see Section I.E.6.), and the Wiretapping and Electronic Surveillance Control Act (WESCA) (18 Pa. Cons. Stat. § 5701 *et seq.*; see Section I.F.). Finally, laws related to privacy and data security applicable to specific sectors, such as health care and insurance, are set forth in the portions of this profile dedicated to those sectors.

1. Who is covered?

Under the Breach of Personal Information Notification Act (BPINA), notification of a breach of the security of an entity's system for storage and management of computerized data must be made to any resident of Pennsylvania whose personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person (73 Pa. Stat. § 2303(a)). For specific information on the form of notification, see Section I.C.8.

2. What is covered?

The Breach of Personal Information Notification Act (BPINA) applies to a "breach of the security of the system," defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by an entity as part of a database of personal information regarding multiple individuals and that causes or is reasonably believed will cause loss or injury to a Pennsylvania resident (73 Pa. Stat. § 2302). "Personal information" is defined as an individual's first name or first initial and last name in combination with and linked to any of the following data elements:

- social security number;
- driver's license number or state ID card; or
- financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302).

BPINA provides an exception to the notification requirement if a law enforcement agency determines that the notification will impede a criminal or civil investigation. Notification must be made after the law enforcement agency determines that notification will not compromise the investigation or national or homeland security (73 Pa. Stat. § 2304).

No notification is required if the data at issue is encrypted, unless the security breach is linked to a breach of the security of the encryption, or the security breach involves a person with access to the encryption key (73 Pa. Stat. § 2303(b)).

For information on notification methods, see Section I.C.8.

3. Who must comply?

The Breach of Personal Information Notification Act (BPINA) requires specific entities to provide notification to Pennsylvania residents concerning breaches of their personal information as described above and at Section I.C.8. An "entity" is defined as a state agency, a political subdivision, or an individual or business doing business in Pennsylvania. "Businesses" include a variety of entity types, such as sole proprietorships, partnerships, corporations, and associations, including financial institutions, as well as any entity that destroys records (73 Pa. Stat. § 2302). In addition, vendors maintaining, storing, or managing computerized data for another entity must provide notice of a breach to the entity, and the entity is then responsible for discharging the duties of the breach notification law (73 Pa. Stat. § 2303(c)). For information on BPINA notification requirements, see Section I.C.8.

C. DATA MANAGEMENT PROVISIONS

1. Notice & Consent

There are no general Pennsylvania laws governing notice and consent requirements with respect to the collection or disclosure of personal information. Sector-specific laws do contain such requirements, including laws governing health data and health care facilities and providers (see Section I.D.9. and Section I.E.5.), employers (see Section I.E.6.), and insurers (see Section I.E.7.). In addition, the Wiretapping and Electronic Surveillance Control Act (WESCA) prohibits recordings of electronic, wire, or oral communications without the consent of all parties to the communication (see Section I.F.). Finally, under the Credit Reporting Agency Act (CRAA), a credit reporting agency may not release information from a security report without prior express authorization from the consumer (see Section I.D.4.).

For information on breach notification requirements under the Breach of Personal Information Notification Act (BPINA), see Section I.C.8.

2. Collection & Use

There are no general Pennsylvania laws governing collection and use requirements regarding personal information. Under the Breach of Personal Information Notification Act (BPINA), the good faith acquisition of personal information by an employee or agent of an entity subject to BPINA breach notification requirements is not considered a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and not subject to further unauthorized disclosure (73 Pa. Stat. § 2302). For more information on BPINA, see Section I.C.8.

Sector-specific laws do contain collection and use requirements, including laws governing health data and health care facilities and providers (see Section I.D.9. and Section I.E.5.), employers (see Section I.E.6.), and insurers (see Section I.E.7.).

3. Disclosure to Third Parties

There are no general Pennsylvania laws governing the disclosure of personal information to third parties. Under the Breach of Personal Information Notification Act (BPINA), the good faith acquisition of personal information by an employee or agent of an entity subject to BPINA breach notification requirements is not considered a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and not subject to further unauthorized disclosure (73 Pa. Stat. § 2302). For more information on BPINA, see Section I.C.8. In addition, the provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) governing stored communications held by electronic communications providers restrict the disclosure of such communications by the provider (see Section I.D.7.).

Sector-specific laws do contain such requirements, including laws governing health data and health care facilities and providers (see Section I.D.9. and Section I.E.5.), employers (see Section I.E.6.), and insurers (see Section I.E.7.).

4. Data Storage

There are no general Pennsylvania laws governing the storage of data containing personal information.

5. Access & Correction

There are no general Pennsylvania laws governing subjects' rights with respect to access to, and correction of, records containing their personal information. However, under the Inspection of Employee Records Law (Personnel Files Act), employers are required to provide employee access to personnel records, and under specified circumstances, the Bureau of Labor Standards of the Department of Labor & Industry may make and enforce an order providing access to records and the opportunity for an employee to place a counter statement in the employee's file in the event an alleged error is determined by the employee.

6. Data Security

There are no general Pennsylvania laws governing the obligations of business regarding the security of data in its possession containing personal information. Insurers are subject to provisions in the Pennsylvania Code establishing standards for safeguarding customer information (see Section I.E.7.).

7. Data Disposal

There are no general Pennsylvania laws governing the obligations of business regarding the disposal of data containing personal information.

8. Data Breach

Under the Breach of Personal Information Notification Act (BPINA), notification of a breach of the security of an entity's system for storage and management of computerized data must be made to any resident of Pennsylvania whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person (73 Pa. Stat. § 2303(a)). Notice also is required if encrypted information is accessed and acquired in an unencrypted form, if the breach is linked to a breach of the security of the encryption, or if it involves a person with access to the encryption key (73 Pa. Stat. § 2303(b)). An “entity” is defined as a state agency, a political subdivision, or an individual or business doing business in Pennsylvania. “Businesses” include a variety of entity types, such as sole proprietorships, partnerships, corporations, and associations, including financial institutions, as well as any entity that destroys records (73 Pa. Stat. § 2302). Vendors maintaining, storing, or managing computerized data for another entity must provide notice of a breach to the entity, and the entity is then responsible for discharging the duties of the breach notification law (73 Pa. Stat. § 2303(c)).

Notification methods: BPINA provides that notice may be provided by any of the following methods:

- written notice to the last known home address;
- telephone notice, if
    - the customer can reasonably be expected to receive it;
    - the notice is given in a clear and conspicuous manner;
    - the notice describes the incident in general terms and verifies personal information but does not require the customer to provide personal information; and
    - the customer is provided with a phone number or website for further information or assistance; or
- e-mail notice, if a prior business relationship exists and the entity has the person's valid e-mail address (73 Pa. Stat. § 2302(1) -(3)).

Substitute notice may be used if the entity can show that the cost of providing notice would exceed $100,000, the affected class exceeds 175,000, or the entity does not have sufficient contact information (73 Pa. Stat. § 2302(4)(i)). Substitute notice must include all of the following:

- e-mail notice where the entity has the subject's e-mail address;

- conspicuous posting on the entity's website if it maintains one; and
- notification to major statewide media (73 Pa. Stat. § 2302(4)(ii)).

Law enforcement exception: BPINA provides an exception to the notification requirement if a law enforcement agency determines that the notification will impede a criminal or civil investigation. Notification must be made after the law enforcement agency determines that notification will not compromise the investigation or national or homeland security (73 Pa. Stat. § 2304).

Exemptions: Entities that maintain their own notification procedure as part of an information privacy and security program that is consistent with the notice requirements of BPINA are exempt from BPINA provided that they notify subjects in accordance with their policy in case of a breach (73 Pa. Stat. § 2307(a)). In addition, financial institutions complying with notification requirements contained in the "Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" are deemed to be in compliance with BPINA, as are entities that comply with notice requirements or procedures pursuant to rules, regulations, and procedures established by the entity's primary federal regulator (73 Pa. Stat. § 2307(b)).

Definitions: A "breach of the security of the system" is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by an entity as part of a database of personal information regarding multiple individuals and that causes or is reasonably believed will cause loss or injury to a Pennsylvania resident (73 Pa. Stat. § 2302). BPINA defines "personal information" as an individual's first name or first initial and last name in combination with and linked to any of the following data elements:

- social security number;
- driver's license number or state ID card; or
- financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302).

Notice to consumer reporting agencies: Any entity providing breach notification under BPINA to more than 1,000 persons at one time must, without unreasonable delay, also notify all consumer reporting agencies compiling and maintaining files on consumers nationwide under the federal Fair Credit Reporting Act of the timing, distribution, and number of notices (73 Pa. Stat. § 2305).

Remedies: Violations of BPINA are deemed to be unfair or deceptive trade practices in violation of the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 201-1 *et seq.*). The Attorney General has the exclusive authority to bring an action under this law (73 Pa. Stat. § 2308). BPINA does not establish a private cause of action for violations.

9. Data Transfer & Cloud Computing

Our research has revealed no provisions of Pennsylvania law generally addressing data transfers or cloud computing. However, 2016 Pa. Laws Act No. 76 established the Pennsylvania eHealth Partnership Program , which is responsible for the creation and maintenance of Pennsylvania's secure health information exchange, known as the PA Patient & Provider Network, or P3N. See 62 Pa. Stat. § 1401-C *et seq.* As for cloud computing, Formal Opinion 2011-200 of the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility notes that an attorney "may ethically allow client confidential material to be stored in 'the cloud' provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks."

10. Other Provisions

There are no other provisions of Pennsylvania law governing data management issues.

D. SPECIFIC TYPES OF DATA

1. Biometric Data

There are no specific Pennsylvania laws addressing the collection and use of biometric information.

2. Consumer Data

Consumer Protection Against Computer Spyware Act: Under the Consumer Protection Against Computer Spyware Act (73 Pa. Stat. § 2330.1 *et seq.*), no person or entity who is not an authorized user (defined as a person who owns or who is authorized by an owner or lessee to use a computer) may—with actual knowledge, conscious avoidance of actual knowledge, or willfully—cause computer software to be copied onto the computer of an authorized user in Pennsylvania with the purpose of modifying computer settings of Internet browsers, page displays, or proxies used to search the Internet; collecting specified personally identifiable information through deceptive means; preventing an authorized user's reasonable efforts to block installation of such software; misrepresenting that such software will be uninstalled; or removing or disabling security, antispyware, or antivirus software on the computer (73 Pa. Stat. § 2330.3). The law also prohibits a person or entity who is not an authorized user from taking control of a computer using specified means, modifying particular settings, or preventing an authorized user's efforts to block such activities (73 Pa. Stat. § 2330.4).

Persons or entities who are not authorized users may not induce an authorized user to install a software component by misrepresenting that the software is necessary for security or privacy reasons to open, view, or play a particular type of content, or cause the copying and execution of such software on the computer (73 Pa. Stat. § 2330.5).

The prohibitions of the law do not apply to activities undertaken by a cable operator, computer hardware or software provider, or provider of an information service or interactive computer service for the purpose of network or computer security, diagnostics, technical support, repair, authorized updates, network management or maintenance, authorized remote system management, or detection and prevention of unauthorized use or fraud. Additionally, the prohibitions do not apply to lawful wiretapping activities under the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.; 73 Pa. Stat. § 2330.6).

Violators are subject to criminal penalties (see Section I.H.), and civil remedies are available for specified persons adversely affected by a violation (see Section I.G.1.).

BPINA: Under the Breach of Personal Information Notification Act (BPINA), “personal information” is defined as an individual's first name or first initial and last name in combination with and linked to data elements such as a social security number, driver's license number or state ID card, or a financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302). Accordingly, any entity maintaining, storing, or managing consumer data in a computerized format that contains such information would be subject to the notification requirements of BPINA if such data is breached. For more information, see Section I.C.8.

3. Credit Card Data

Under the Breach of Personal Information Notification Act (BPINA), “personal information” is defined as an individual's first name or first initial and last name in combination with and linked to data elements such as a social security number, driver's license number or state ID card, or a financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302). Accordingly, any entity maintaining, storing, or managing credit card data in a computerized format that contains such personal information would be subject to the notification requirements of BPINA if such data is breached. For more information, see Section I.C.8.

4. Credit Reports

Credit Reporting Agency Act: Under the Credit Reporting Agency Act (CRAA) (73 Pa. Stat. § 2501 *et seq.*), consumers may elect to place a security freeze on their credit reports by providing proper identification to a consumer reporting agency. The request may be made via certified mail or through a secure Internet connection (73 Pa. Stat. § 2503(a)(1)). The reporting agency must place the freeze no later than five days after receiving a request (73 Pa. Stat. § 2503(a)(3)). The agency may impose a reasonable fee to place the freeze, but such fee may not exceed $10, and fees for a request to temporarily lift a freeze may not exceed $10 per request. No fee may ever be charged for removing a freeze (73 Pa. Stat. § 2509(a)). The law provides an exception to charging fees for consumers who are victims of identity theft or who are age 65 or older (73 Pa. Stat. § 2509(b)). If a security freeze is in

place, a consumer reporting agency cannot change information regarding a consumer's name, date of birth, social security number, or address without sending written confirmation of the change to the consumer within 30 days of the change. Technical corrections do not require written confirmation, but in the case of an address change, the confirmation must be sent to both the new address and former address (73 Pa. Stat. § 2509(c)).

Certain entities, such as check services or fraud prevention services companies or deposit account information services companies, are not required to place a security freeze, provided specified conditions are met (73 Pa. Stat. § 2503(a)(4)). In addition, the law provides that certain entities may receive a consumer report regardless of a freeze, including federal, state, and local government entities; private collections agencies or persons holding a financial obligation of the consumer; child support enforcement agencies; and other entities, under specified circumstances (73 Pa. Stat. § 2503(e)).

Once a freeze is in place, a credit reporting agency may not release information from a security report without prior express authorization from the consumer, although the agency may inform the third party that a freeze is in effect (73 Pa. Stat. § 2503(b) and 73 Pa. Stat. § 2506). The freeze must remain in place until the earlier of the date an agency receives a request from the consumer to remove the freeze or seven years after the date the freeze was initiated (73 Pa. Stat. § 2503(d)). Within 10 business days of a request for a freeze, the consumer reporting agency must send the consumer a written confirmation with a unique personal identification number or password that the consumer may use to provide authorization for access to the consumer's report, as well as written notification to the consumer on procedures for removing or temporarily lifting the freeze or allowing access for specific parties or for a specific period (73 Pa. Stat. § 2504). The law places specific requirements on consumers who seek to remove a freeze or to allow temporary access to a consumer report (73 Pa. Stat. § 2507). Consumers may request a replacement personal identification number or password (73 Pa. Stat. § 2505).

Consumer reporting agencies may develop secure procedures using telephone, fax, Internet, or other electronic media to receive and process requests for security freezes under the CRAA (73 Pa. Stat. § 2508).

Violations of the CRAA are deemed to be unfair or deceptive trade practices in violation of the Unfair Trade Practices and Consumer Protection Law. The Attorney General has the exclusive authority to bring an action under this law for violations of the CRAA (73 Pa. Stat. § 2510).

BPINA: Under the Breach of Personal Information Notification Act (BPINA), “personal information” is defined as an individual's first name or first initial and last name in combination with and linked to data elements such as a social security number, driver's license number or state ID card, or a financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302). Accordingly, any entity maintaining, storing, or managing credit report data in a computerized format that contains such personal information would be subject to the notification requirements of BPINA if such data is breached. For more information, see Section I.C.8.

5. Criminal Records

In general, an employer may inquire into criminal background information. Under provisions of the Criminal Code governing dissemination of criminal history information, before a state or local police department may disseminate such information, it must extract all notations of arrests, indictments, or other information related to the initiation of criminal proceedings where three years have lapsed from the arrest date, no conviction has occurred, and no proceedings are pending seeking a conviction (18 Pa. Cons. Stat. § 9121(b)(2)). An employer may only consider felony and misdemeanor convictions on an applicant's criminal history, and only then to the extent that they relate to the applicant's suitability for employment in the position for which the applicant applied (18 Pa. Cons. Stat. § 9125(a) -(b)). The employer must provide an applicant with written notification if the decision not to hire is based in whole or in part on the applicant's criminal history information (18 Pa. Cons. Stat. § 9125(c)). A person aggrieved by a violation of the above provisions may bring an action for injunctive relief or damages (see Section II.C. and Section I.G.4.).

Under regulations administered by the Public Utility Commission, common or contract carriers may not permit a person to operate a vehicle until they have obtained and reviewed a criminal history from the Pennsylvania State Police and every other state in which the person has resided for the past 12 months. Following receipt of the initial criminal history record, the common or contract carrier must obtain and review a criminal history record for each driver in its employ from the Pennsylvania State Police every two years from the date of the last report. A common or contract carrier may not permit a person to operate a vehicle if the person has been convicted of a felony or misdemeanor under the laws of Pennsylvania or another jurisdiction, to the extent that the conviction relates adversely to the person's suitability to provide safe and legal service. The common or contract carrier must maintain a copy of the criminal history for at least three years (52 Pa. Code § 29.505).

Specified applicants for employment with a child-care provider must provide a criminal history report from the Pennsylvania State Police or a statement to the effect that there is no such information on the applicant, a certification from the Department of Public Welfare stating whether the applicant has been named in the central register as the perpetrator of a founded or indicated report of child abuse, and a report of federal criminal history record information obtained from the FBI using fingerprints (23 Pa. Cons. Stat. § 6344). Similar provisions apply to prospective applicants for jobs in public and private schools (24 Pa. Stat. § 1-111).

6. Drivers' Licenses/Motor Vehicle Records

Under regulations administered by the Public Utility Commission, common or contract carriers may not permit a person to operate a vehicle until they have obtained and reviewed a driver history from the appropriate agency of every state in which the person held a motor vehicle operator's license or permit during the preceding three years. Following receipt of the initial driver report, the common or contract carrier must obtain a driver history for each driver in its employ from the appropriate agency of the state in which the driver held an operator's license at least once every 12 months from the date of the last report. The common or contract carrier must maintain a copy of the driver history for at least two years (52 Pa. Code § 29.504).

Common or contract carriers are also required to obtain a criminal history record for drivers (see Section I.D.5.).

7. Electronic Communications/Social Media Accounts

Under the Wiretapping and Electronic Surveillance Control Act (WESCA), a person or entity providing an electronic communication service to the public may not knowingly divulge to any person or entity the contents of an electronic communication in the electronic storage of the service on behalf of a subscriber or customer if the communication was received solely for the purpose of providing storage or computer processing services to the subscriber or customer and if the service provider is not authorized to access the communication for any purpose other than storage or computer processing (18 Pa. Cons. Stat. § 5742(a)(1)). A similar prohibition applies to remote computing service providers (18 Pa. Cons. Stat. § 5742(a)(2)). Exceptions are provided for disclosures to the intended recipient, disclosures made with the consent of the originator of the communication or subscriber to the remote computing service, and to law enforcement officials under certain circumstances, among others (18 Pa. Cons. Stat. § 5742(b) -(c)). Persons aggrieved by a knowing violation of these provisions have a civil cause of action (18 Pa. Cons. Stat. § 5747; see Section I.G.4.).

Any person who provides e-mail service or a wireless telecommunication company may block or filter the receipt or transmission through its service of any commercial e-mail or wireless advertisement that it reasonably believes is or may be sent in violation of the state's anti-spam law (73 Pa. Stat. § 2250.6). For more information on the anti-spam law, see Section I.E.1.

8. Financial Information

Provisions of the Pennsylvania Code's title governing insurance (31 Pa. Code § 146a.1 *et seq.*) contain a variety of requirements with respect to nonpublic financial information that insurance providers licensed in Pennsylvania must meet, including notice and disclosure requirements. For detailed information on these provisions, see Section I.E.7.

Under the Breach of Personal Information Notification Act (BPINA), “personal information” is defined as an individual's first name or first initial and last name in combination with and linked to data

elements such as a social security number, driver's license number or state ID card, or a financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302). Accordingly, any entity maintaining, storing, or managing consumer data in a computerized format that contains such information would be subject to the notification requirements of BPINA if such data is breached. For more information, see Section I.C.8.

Provisions of Pennsylvania law governing the privacy of social security numbers (74 Pa. Stat. § 201 *et seq.*; see Section I.D.10.) do not apply to financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA) (74 Pa. Stat. § 204).

9. Health Data

Access to patient records: Under provisions of Pennsylvania law governing the rules of evidence, a patient or his designee, including his attorney, has the right to access the patient's medical charts or records and to obtain photocopies of them for the patient's use, without obtaining a subpoena. A health care provider or facility may charge a fee for such records, but not in excess of the fee amounts set forth at 42 Pa. Cons. Stat. § 6152(a)(2)(i) and as adjusted for inflation (42 Pa. Cons. Stat. § 6155(b)). If a medical chart or record is requested for purposes of supporting a claim or appeal under the federal Social Security Act or any federal or state financial need-based benefit program, a health care facility may only charge a flat fee that is adjusted annually. For 2017, the fee is $27.92 (Department of Health Notice, 46 Pa. B. 7598, Dec. 3, 2016). This notice also sets out the current fee schedule for copies of medical records.

Confidentiality and disclosure of records held by managed care plans: Managed care plans (including HMOs) and utilization review entities must adopt and maintain procedures to ensure that all identifiable information regarding enrollee health, diagnosis, and treatment is adequately protected and remains confidential (40 Pa. Stat. § 991.2131(a)). Such entities also must adopt and maintain procedures to ensure that enrollees have timely access to their medical records unless prohibited by federal or state law or regulation (40 Pa. Stat. § 991.2131(b)). An entity must make information on an enrollee's health or treatment available to the enrollee or his designee, and the law provides for disclosure of identifiable information in specified circumstances, such as to determine coverage or facilitate payment of a claim, or to a public official charged with enforcing compliance in the course of his duties, among others. If a disclosure is made for the purposes of patient care management, outcomes improvement, or research, an enrollee must provide consent, and the identity of the enrollee must remain anonymous to the greatest extent possible (40 Pa. Stat. § 991.2131(c)). The Department of Health or the Insurance Department, as appropriate, may impose a civil penalty of up to $5,000 for any violation of these provisions.

Cancer and communicable disease reporting: Hospitals and laboratories must report cases of cancer to the Department of Health, but the reports so submitted are confidential and not subject to public inspection or dissemination (35 Pa. Stat. § 5636).

Physicians must report persons who have or are suspected of having a communicable disease to the local board or department of health serving the municipality where the disease occurred (35 Pa. Stat. § 521.4). Provisions of the Pennsylvania Code extend this requirement to clinical laboratories, health care practitioners, health care facilities, orphanages, child care group settings, and institutions maintaining dormitories or living rooms (28 Pa. Code § 27.21a through 28 Pa. Code § 27.23). The information contained in such records may not be disclosed to any person who is not a member of the Department of Health or a local board or department (35 Pa. Stat. § 521.15).

HIV-related information: Under the Confidentiality of HIV-Related Information Act (35 Pa. Stat. § 7601 *et seq.*), no person who obtains confidential HIV-related information in the course of providing any health or social service or pursuant to a patient's authorization may disclose the information without the written consent of the patient, except to specifically designated individuals, including the subject, the physician who ordered the test, and other designated health care providers, insurers, and public officials (35 Pa. Stat. § 7607(a)). The law specifies the required elements to be included in the written consent, including names of the parties, the purpose of the disclosure, and the type of information to be disclosed (35 Pa. Stat. § 7607(c)). A person whose HIV-related information has been disclosed in violation of these provisions may bring a private cause of action (35 Pa. Stat. § 7610; see I.G.4.).

Mental health documents: All documents concerning persons in mental health treatment are confidential and may not be released without the person's consent, except to those engaged in the person's treatment, to a county administrator under specified circumstances, in the course of authorized legal proceedings, or pursuant to specified federal rules. Privileged written or oral communications may not be disclosed at any time without written consent (50 Pa. Stat. § 7111). Regulations provide further requirements with respect to the confidentiality of mental health records (55 Pa. Code § 5100.31 *et seq.*). Similarly, it is a criminal misdemeanor "for any person to disclose without authority the contents of any records or reports touching upon any matter concerning a person who has been admitted, committed or detained pursuant to the provisions of [the Mental Health and Intellectual Disability Act (50 Pa. Stat. § 4101 *et seq.*)]" (50 Pa. Stat. § 4605(5)).

Drug and alcohol treatment records: All patient records prepared or obtained pursuant to state and local programs for treatment under the Pennsylvania Drug and Alcohol Abuse Control Act (71 Pa. Stat. § 1690.101 *et seq.*) must remain confidential and may be disclosed only with the patient's consent and only to specified medical personnel or government officials, although exceptions are provided for emergency medical situations and disclosures pursuant to court order (71 Pa. Stat. § 1690.108(b)). Similar restrictions apply to patient records prepared or maintained by a private practitioner, hospital, clinic, or drug rehabilitation or drug treatment center, but there is no provision for such a private entity to disclose such information pursuant to court order (71 Pa. Stat. § 1690.108(c)).

Provisions regarding minors: See Section I.D.12.

Insurance Code provisions: Provisions of the Pennsylvania Code's title governing insurance (31 Pa. Code Ch. 146b) contain a variety of requirements with respect to nonpublic health information that insurance providers licensed in Pennsylvania must meet, including notice and disclosure requirements. For detailed information on these provisions, see Section I.E.7.

10. Social Security Numbers

The privacy of social security numbers (SSN) in Pennsylvania is governed by 74 Pa. Stat. § 201 *et seq.*). No person, entity, state agency, or political subdivision may do any of the following:

- publicly post or display an SSN;
- print an individual's SSN on any card required for the individual to access products or services;
- require an individual to transmit an SSN over the Internet unless the connection is secure or the SSN is encrypted;
- require an individual to use an SSN to access a website unless a password or other unique identifier is also required for access;
- print an individual's SSN on any material mailed to the individual unless required by federal or state law (although SSNs may be included in an application or form sent by mail under certain circumstances, but for such inclusion to be allowed, the SSN must not be visible without an envelope having been opened); and
- disclose in any manner an SSN of an individual applying for a recreational fish or game license except to the agency issuing the license.

The prohibitions regarding SSNs do not apply to financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA) or to entities covered under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Fair Credit Reporting Act (74 Pa. Stat. § 204).

Actions violating the requirements outlined above are considered summary offenses subject to a fine (74 Pa. Stat. § 201(g); see Section II.C.). Both district attorneys and the Attorney General are authorized to investigate and institute criminal proceedings for violations (74 Pa. Stat. § 202; see Section I.H.).

11. Usernames & Passwords

Under the Breach of Personal Information Notification Act (BPINA), "personal information" is defined as an individual's first name or first initial and last name in combination with and linked to data elements such as a social security number, driver's license number or state ID card, or a financial account number or credit or debit card number, in combination with a required security or access code or password permitting access to an individual's financial account (73 Pa. Stat. § 2302). Accordingly,

any entity maintaining, storing, or managing consumer data in a computerized format that contains such information would be subject to the notification requirements of BPINA if such data is breached. For more information, see Section I.C.8.

Pennsylvania's anti-hacking law makes it a felony of the third degree to “intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network, computer database, World Wide Web site or telecommunication device” (18 Pa. Cons. Stat. § 7611(a)(3)).

12. Information about Minors

When a parent or legal guardian has consented to the inpatient or outpatient mental health treatment of a minor age 14 or older, the parent or legal guardian may consent to the release of the minor's medical records and information, including records from prior treatment to which the minor had provided consent, to the minor's current mental health care provider. In addition, the parent or guardian may consent to the release of mental health care records to the primary care provider provided that the mental health care provider determines that such release will not be detrimental to the minor (35 Pa. Stat. § 10101.2(a) -(c)). In other instances, a minor age 14 or older controls the release of his mental health treatment records and information to the extent allowed by law (35 Pa. Stat. § 10101.2(d)).

Under regulations governing the confidentiality of health records, if a client or patient is under the age of 14, control over the release of records may be exercised by a parent or guardian (55 Pa. Code § 5100.33(a)).

Many of the requirements regarding the confidentiality of health data and required consent of the data subject prior to disclosure, including drug and alcohol treatment records and HIV-related records and information, are applicable to minors (see Section I.D.9.).

Information received in confidence from a student may be revealed to the student's parent or guardian or a principal or other appropriate authority when the health, safety, or welfare of the student or another person is clearly in jeopardy (22 Pa. Code § 12.12).

13. Location Data

Under certain specified circumstances, law enforcement officials may obtain an order for the installation and use of mobile tracking devices (18 Pa. Cons. Stat. § 5761; see Section I.F.).

14. Other Personal Data

Our research has uncovered no other Pennsylvania state law provisions regarding personal data beyond those specified above.

E. SECTOR-SPECIFIC PROVISIONS

1. Advertising & Marketing

Anti-spam law: Under the Unsolicited Telecommunication Advertising Act (73 Pa. Stat. § 2250.1 *et seq.*), no person may initiate a transmission or conspire with another person to initiate a transmission of an unsolicited commercial e-mail or fax from a computer or fax machine located in Pennsylvania or to an e-mail address that does any of the following:

- uses a third party's Internet domain name in the return e-mail message without permission of the third party;
- includes false or misleading information in the return address portion of the e-mail, fax, or wireless advertisement such that a recipient would be unable to send a reply to the original authentic sender;
- contains false or misleading information in the subject line; or
- fails to operate a valid sender-operated return e-mail address or toll-free phone number that the recipient may use to notify the sender not to send further unsolicited documents (73 Pa. Stat. § 2250.3(a)).

In addition, no person may use a covered mobile telephone messaging system to transmit an unsolicited commercial e-mail (73 Pa. Stat. § 2250.3(b)).

The law prohibits other conduct associated with the sending of commercial e-mails, faxes, and wireless advertisements, including conspiring to initiate a transmission that misrepresents or obscures the point of origin of the transmission; falsifying or forging specified routing information; assisting in a transmission when the person providing the assistance knows the initiator intends to violate the law; removing or disabling any data, programs, software, or network to initiate a commercial e-mail or fax; or selling, distributing, or possessing software used for the purpose of falsifying commercial e-mail or fax transmissions (73 Pa. Stat. § 2250.4).

Violations of the law constitute a violation of the Unfair Trade Practices and Consumer Protection Law, and the Attorney General may take action to enforce the law subject to administrative law and procedure requirements concerning notice, hearing, and the right of appeal (73 Pa. Stat. § 2250.5). The law further provides for consumer remedies under the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 2250.7).

In addition to the remedies provided above, consumers may make a complaint regarding violations of the law with the Attorney General's Bureau of Consumer Protection. If, after an investigation, a violation is found, the Attorney General may bring an action for a civil penalty and other relief (73 Pa. Stat. § 2250.8; see Section I.G.1.).

It should be noted 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).

BPINA: The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the advertising and marketing sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

WESCA: Personnel engaged in telephone marketing or customer service may intercept oral communications without violating the provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.), if the business only uses the intercepted communication for training, quality control, and monitoring and one party to the communication has consented to the interception (18 Pa. Cons. Stat. § 5704(15)).

Do-not-call provisions: Under the Telemarketer Registration Act (73 Pa. Stat. § 2241 *et seq.*), telemarketers are prohibited from initiating an outbound call to a person when the person has previously stated that he does not wish to receive such a call (73 Pa. Stat. § 2245(2)). In addition, no telemarketer may make a call to the number of a residential telephone subscriber who has placed his name, address, and phone number to be enrolled on a do-not-call list maintained by a list administrator. A listing on the do-not-call list must be maintained for a minimum of five years (73 Pa. Stat. § 2245.2).

Consumers may make a complaint regarding violations of the law with the Attorney General's Bureau of Consumer Protection. If, after an investigation, a violation is found, the Attorney General may bring an action for a civil penalty and other relief under the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 201-1 *et seq.*). The Attorney General must remit 10% of any civil penalty to the person filing the complaint, but the amount so remitted may not exceed $100 for any one person (73 Pa. Stat. § 2245.2(k)). In addition, the Attorney General may seek revocation of a telemarketer's registration on a second or subsequent violation (73 Pa. Stat. § 2246(b)).

2. Education

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the education sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts,

and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the education sector.

Information received in confidence from a student may be revealed to the student's parent or guardian or a principal or other appropriate authority when the health, safety, or welfare of the student or another person is clearly in jeopardy (22 Pa. Code § 12.12).

3. Electronic Commerce

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the electronic commerce sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the electronic commerce sector. However, personnel engaged in customer service may intercept oral communications without violating WESCA if the business only uses the intercepted communication for training, quality control, and monitoring and one party to the communication has consented to the interception (18 Pa. Cons. Stat. § 5704(15)).

4. Financial Services

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the financial services sector maintaining, storing, or managing such data. However, financial institutions complying with notification requirements contained in the "Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" are deemed to be in compliance with BPINA (73 Pa. Stat. § 2307(b)). For more information on BPINA, see Section I.C.8.

Financial institutions subject to the federal Gramm-Leach-Bliley Act (GLBA) are not subject to provisions making it a deceptive or fraudulent business practice to make a false or misleading statement in a privacy policy (18 Pa. Cons. Stat. § 4107(c); see Section I.H.).

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the financial services sector.

5. Health Care

A variety of laws governing specific health care data and entities that collect and maintain records containing such data require specified entities to maintain the confidentiality of such records and restrict their disclosure. For more information, see Section I.D.9.

Entities covered under the federal Health Insurance Portability and Accountability Act (HIPAA) are not subject to provisions making it a deceptive or fraudulent business practice to make a false or misleading statement in a privacy policy (18 Pa. Cons. Stat. § 4107(c); see Section I.H.).

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the health care sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the health care sector.

6. HR & Employment

Personnel Files Act: The Inspection of Employee Records Law (Personnel Files Act) (43 Pa. Stat. § 1321 *et seq.*) governs employer's obligations with respect to making personnel records available to employees. The law defines an "employee" to include any person currently employed, laid off with reemployment rights, or on leave of absence, but the term does not include applicants for employment (43 Pa. Stat. § 1321). "Personnel files" include applications for employment; wage and salary information; notice of commendation, warning, or discipline; specified tax and fringe benefit information; leave records; and employment history, including attendance records and employment evaluations. The term does not include records relating to an investigation of a criminal offense; letters of reference; documents being developed for use in a civil, criminal, or grievance procedure; medical records used by the employer to plan for future operations; or information available to the employee under the federal Fair Credit Reporting Act (43 Pa. Stat. § 1321).

On employee request, an employer must, at reasonable times, permit the employee or an agent to inspect personnel files used to determine an employee's qualifications for employment, promotion, additional compensation, termination, or disciplinary action. The records must be available during regular business hours in the office in which they are usually maintained, and sufficient time during the course of a regular business day must be available for the inspection. Employers may require employees to inspect the records on their free time and may require employees to submit a written form requesting access or designating an agent for purposes of access and inspection. Such a form is only to be used for the purpose of identifying the employee or an agent to avoid improper disclosure. In a written request, an employee should indicate either the purpose for which the inspection is requested or the particular parts of the record the employee or agent wishes to inspect (43 Pa. Stat. § 1322). When designating an agent to inspect records, an employee must provide the employer with a signed authorization identifying the specific individual authorized to inspect the file (43 Pa. Stat. § 1322.1).

The Personnel Files Act does not require that an employee be permitted to remove all or part of a personnel file or a copy thereof from the employer's premises, although the employee or agent may take notes during an inspection. An employer may require that files be inspected in the presence of an official designated by the employer and retains the right to protect files from loss, damage, or alteration to insure file integrity. The employer must allow sufficient inspection time depending on the volume of the file. Employers may limit inspections to once a year by an employee and once a year by an employee's agent, except for reasonable cause (43 Pa. Stat. § 1323).

Upon petition from either an employer or an employee, the Bureau of Labor Standards of the Department of Labor & Industry may make and enforce an order under the Personnel Files Act that, as appropriate, will provide access to records and the opportunity for an employee to place a counter statement in the employee's file in the event an alleged error is determined by the employee. Employees must avail themselves of all civil remedies (i.e., a grievance procedure) under a union contract (43 Pa. Stat. § 1324).

BPINA: The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to employers maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

WESCA: Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock

companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions apply to employers.

7. Insurance

Privacy of consumer financial information: Provisions of the Pennsylvania Code's title governing insurance (31 Pa. Code § 146a.1 *et seq.*) contain a variety of requirements with respect to nonpublic financial information that insurance providers licensed in Pennsylvania must meet, as outlined below.

Notice: A licensee must provide initial notice of its privacy policies and practices to a customer at the time that the customer relationship is established or to a consumer before the licensee makes any disclosure of nonpublic financial information about the consumer to a nonaffiliated third party. A customer relationship is established when a consumer becomes a policy holder or agrees to obtain financial, economic, or investment advisory services from a licensee (31 Pa. Code § 146a.11). Annual notices of privacy policies and procedures must be given to customers, although notice to terminated customers is not required (31 Pa. Code § 146a.12). The Code specifies the information to be included in the notice (31 Pa. Code § 146a.13) and the method of delivery (31 Pa. Code § 146a.16).

Disclosure limitations and opt-out procedures: A licensee may not disclose nonpublic personal information to a nonaffiliated third party unless it meets all of the following conditions:

- The licensee has provided the initial notice described above;
- The licensee has provided an opt-out notice as described below;
- The licensee has given the consumer a reasonable opportunity to opt out prior to disclosing the information; and
- The consumer does not opt out (31 Pa. Code § 146a.21(a)).

Licensees required to give an opt-out notice as described above must provide a clear and conspicuous notice to consumers stating that the licensee discloses or reserves the right to disclose nonpublic financial information to a nonaffiliated third party and that the consumer has the right to opt out, together with a reasonable means for the customer to opt out (31 Pa. Code § 146a.14). The law describes circumstances constituting reasonable means, including by mail or electronic means or as part of an isolated transaction with a customer (31 Pa. Code § 146a.21(c)). Licensees may allow consumers to partially opt out of disclosures (31 Pa. Code § 146a.21(e)).

Exceptions to limits on disclosures and opt-out requirements: Licensees are not required to provide notice of opt-out procedures or to limit their disclosure of nonpublic financial information if the disclosure is made to a nonaffiliated third party to perform services or functions on the licensee's behalf, or if the licensee provided initial notice to the consumer and enters into a contractual agreement with the third party prohibiting it from disclosing or using the information other than for the purposes that the licensee disclosed the information (31 Pa. Code § 146a.31). Other exceptions apply for disclosures necessary to effectuate a transaction requested by the consumer (31 Pa. Code § 146a.32) or to disclosures made with the consent of the consumer, to protect confidentiality of the licensee's records, or for the purpose of fraud prevention or resolving customer disputes, among others (31 Pa. Code § 146a.33).

Violations: A violation of these provisions is considered to be an unfair method of competition and an unfair or deceptive act or practice and is subject to any applicable remedies under the Unfair Insurance Practices Act (40 Pa. Stat. § 1171.1 *et seq.*; see Section II.C.) (31 Pa. Code § 146a.43).

Privacy of consumer health information: Provisions of the Pennsylvania Code's title governing insurance (31 Pa. Code § 146b.1 *et seq.*) contain specific requirements with respect to nonpublic health information that insurance providers licensed in Pennsylvania must meet, as outlined below.

Limitations on disclosure: A licensee may not disclose nonpublic personal health information about a consumer unless authorization is obtained from the consumer (31 Pa. Code § 146b.11(a)). Such disclosures are permitted when made for a variety of specified purposes, including claims administration, claims adjustment, fraud prevention and detection, underwriting, risk and case management, and quality control, among others (31 Pa. Code § 146b.11(b)). Disclosures may be made to a third party not licensed by the Department of Insurance provided that the nonpublic health information is disclosed only for one of the insurance functions for which disclosures are permitted, but the licensee may be responsible for any disclosure by the third party that violates the limitation (31 Pa.

Code § 146b.11(d)). The code specifies the contents of a valid authorization, its duration, and the process for revoking an authorization (31 Pa. Code § 146b.12), as well as procedures for delivery of an authorization form (31 Pa. Code § 146b.13).

Violations: A violation of these provisions is considered to be an unfair method of competition and an unfair or deceptive act or practice and is subject to any applicable remedies under the Unfair Insurance Practices Act (40 Pa. Stat. § 1171.1 *et seq.*; see Section II.C.) (31 Pa. Code § 146b.23).

Safeguarding customer information: Insurance licensees are required to implement a comprehensive written information security program including safeguards for the protection of customer information, appropriate to the size and complexity of the licensee and the scope of its activities (31 Pa. Code § 146c.3). The program must safeguard the security and confidentiality of customer information, protect against reasonably anticipated threats to the security or integrity of the information, and protect against unauthorized access or use of information that could result in substantial harm or inconvenience for the customer (31 Pa. Code § 146c.4). The code includes examples of methods of development and implementation of the program, including risk assessment and management, oversight of service provider arrangements, and adjustments to the program (31 Pa. Code § 146c.5 through 31 Pa. Code § 146c.9).

A violation of these code provisions is considered to be an unfair method of competition and an unfair or deceptive act or practice and is subject to any applicable remedies under the Unfair Insurance Practices Act (40 Pa. Stat. § 1171.1 *et seq.*; see Section II.C.). A licensee that knew or should have known of a violation by a service provider of provisions related to these safeguarding provisions, or to the limitations on disclosure of nonpublic financial or health information (see above), is deemed to be in violation unless the licensee took reasonable steps to end the service provider's violation and, if such steps were unsuccessful, either terminated its contract with the service provider or reported the violation to the Department of Insurance if termination is not feasible (31 Pa. Code § 146c.10).

BPINA: The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to insurers maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

WESCA: Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the insurance sector.

8. Retail & Consumer Products

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the retail and consumer products sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the retail and consumer products sector. However, personnel engaged in customer service may intercept oral communications without violating WESCA if the business only uses the intercepted communication for training, quality control, and monitoring and one party to the communication has consented to the interception (18 Pa. Cons. Stat. § 5704(15)).

9. Social Media

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the social media sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the social media sector.

10. Tech & Telecom

Under the Telephone Subscriber Directory Express Consent Act (73 Pa. Stat. § 2401 *et seq.*), a commercial mobile service provider or any direct or indirect affiliate or agent of a provider or any other person in Pennsylvania may not publish in a directory, or provide for publication in a directory, the name and telephone number of any mobile service customer in Pennsylvania without the express consent of the customer. Consent must be given in one of the following ways:

- in writing in a separate document or a distinct section within a written document that includes the customer's signature and the date;
- in a distinct verbal communication from a person sufficiently identified as the customer;
- on a website maintained by the provider providing a separate screen or a separate section of a screen including the disclosure; or
- other verifiable means, including the customer's handset (73 Pa. Stat. § 2403).

Consent may be revoked at any time, and providers must comply with a subscriber's request to opt out within a reasonable time, not to exceed 60 days. Where applicable, the provider must include a disclosure that a customer consenting to be in a directory may incur additional charges for unsolicited calls and text messages (73 Pa. Stat. § 2403).

The Act does not apply to the provision of telephone numbers to collection agencies solely for the collection of unpaid debts to the provider, to specified law enforcement and other public agencies, to a telephone corporation supplying service between service areas for purposes of that corporation's billing services, or to such a corporation to assist in transferring the customer's phone number from an existing or a new provider (73 Pa. Stat. § 2406).

A violation of the act is deemed to be an unfair or deceptive act or practice (73 Pa. Stat. § 2407; see Section II.C.).

The Breach of Personal Information Notification Act (BPINA) applies to an individual or business doing business in Pennsylvania that maintains, stores, or manages computerized data containing personal information (73 Pa. Stat. § 2302 and 73 Pa. Stat. § 2303). Accordingly, BPINA's breach notification requirements apply to businesses in the tech and telecom sector maintaining, storing, or managing such data. For more information on BPINA, see Section I.C.8.

Provisions of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) prohibiting the interception of the wire, electronic, or oral communication of another, or the disclosure or use of information in such a communication, without the consent of all parties to the communication apply to all persons, including individuals, partnerships, associations, joint stock companies, trusts, and corporations (18 Pa. Cons. Stat. § 5702). Accordingly, WESCA's provisions would apply to businesses operating in the tech and telecom sector.

11. Other Sectors

There are no provisions regarding privacy and data security related to other business sectors.

F. ELECTRONIC SURVEILLANCE

Wire, electronic, or oral communications: Electronic surveillance in Pennsylvania is governed by the Wiretapping and Electronic Surveillance Control Act (WESCA), 18 Pa. Cons. Stat. § 5701 *et seq.*). In general, it is a third-degree felony for any person to:

- intentionally intercept, endeavor to intercept, or procure another person to intercept a wire, electronic, or oral communication;
- intentionally disclose or endeavor to disclose to another person the contents of such a communication; or
- intentionally use or endeavor to use the contents of, or evidence derived from, such a communication (18 Pa. Cons. Stat. § 5703).

It is important to note, however, that the interception of a wire, electronic, or oral communication is not illegal if all parties to the communication have given prior consent to the interception (18 Pa. Cons. Stat. § 5704(4)). In addition, WESCA defines the term “oral communication” to mean any such communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying the expectation (18 Pa. Cons. Stat. § 5702). Accordingly, there does not appear to be a prohibition against a recording of a conversation in a public place.

In addition to the all-party-consent exception, WESCA provides numerous exceptions to the prohibition, most of them related to law enforcement activities or to public utilities or electronic communication service providers (18 Pa. Cons. Stat. § 5704). Personnel engaged in telephone marketing or customer service may intercept oral communications if the business only uses the intercepted communication for training, quality control, and monitoring and one party to the communication has consented to the interception (18 Pa. Cons. Stat. § 5704(15)). In addition, WESCA permits recording of conversations between users and contractors with respect to excavation or demolition work if the user informs the parties to the conversation that the call is being recorded (18 Pa. Cons. Stat. § 5704(7)).

WESCA provides that the possession, sale, distribution, or manufacture of electronic, mechanical, or other devices known to be primarily useful for the surreptitious interception of wire, electronic, or oral communication is a third-degree felony (18 Pa. Cons. Stat. § 5705). Exceptions apply to providers of wire or electronic communications services that possess, sell, distribute, or manufacture devices in the normal course of their business and to public entities such as state and local political subdivisions who engage in such activities in furtherance of appropriate public activities (18 Pa. Cons. Stat. § 5706(a)).

Any wire, electronic, or oral communication lawfully intercepted under WESCA must be recorded by tape or other comparable method, and the recording must be done in a manner that protects it from editing or other alteration. If an interception is being monitored, the monitoring must be done by a certified investigative or law enforcement officer. When practicable, such officer must keep a signed written record that includes the date and hours of surveillance; the time and duration of each intercepted communication; the participant in each intercepted conversation, when known; and a summary of each communication's content (18 Pa. Cons. Stat. § 5714).

A person whose wire, electronic, or oral communication is intercepted in violation of WESCA has a civil cause of action against the person committing the violation (18 Pa. Cons. Stat. § 5725; see Section I.G.4.), and the Attorney General may seek an injunction for known or potential violations (18 Pa. Cons. Stat. § 5728; see Section II.C.).

Stored communications: WESCA contains specific provisions prohibiting providers of electronic communications services from divulging the contents of electronic communications in the provider's electronic storage. For details on these provisions, see Section I.D.7.

Mobile tracking devices and other interception devices: A court of common pleas may issue an order for the installation and use of a mobile tracking device under specified circumstances. The law specifies the requirements for the issuance of an order, as well as notice requirements and provisions regarding the removal or movement of the device (18 Pa. Cons. Stat. § 5761). WESCA also prohibits the use of other tracking devices—including pen registers, trap and trace devices, and telecommunication identification interception devices—without a court order, unless an exception applies (18 Pa. Cons. Stat. § 5771 through 18 Pa. Cons. Stat. § 5775).

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Violations of the Breach of Personal Information Notification Act (BPINA) are deemed to be unfair or deceptive trade practices in violation of the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 201-1 *et seq.*). The Attorney General has the exclusive authority to bring an action under this law (73 Pa. Stat. § 2308). BPINA does not establish a private cause of action for violations.

Pennsylvania's anti-spam law (see Section I.E.1.) provides for consumer remedies under the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 2250.7). In addition, consumers may make a complaint regarding violations of the law with the Attorney General's Bureau of Consumer Protection. If, after an investigation, a violation is found, the Attorney General may bring an action for a civil penalty and other relief. The Attorney General must remit 10% of any civil penalty to the person filing the complaint, but the amount so remitted may not exceed $100 (73 Pa. Stat. § 2250.8(a)(1) -(2)). Internet access providers, e-mail service providers, and wireless telecommunications companies aggrieved by a violation of the anti-spam law may initiate an action to enjoin a violation and to recover damages of between $1 and $10 per violation. Each unsolicited commercial e-mail, fax, or wireless communication constitutes a separate violation (73 Pa. Stat. § 2250.8(a)(3)). For willful violations, a court may increase the amount of the reward to an amount not to exceed $1.5 million. In all cases, a court also may award reasonable attorney fees and costs (73 Pa. Stat. § 2250.8(a)(3)(i) -(ii)).

A civil action for violations of the Consumer Protection Against Computer Spyware Act (see Section I.D.2.) may be brought by a provider of computer software adversely affected by the violation, an Internet service provider (ISP) adversely affected by the violation, or a trademark owner whose trademark is used without authorization to deceive users in any deceptive practices prohibited by the law (73 Pa. Stat. § 2330.9(a)). In addition to any other remedies provided by law, such a person may seek injunctive relief, recover damages in an amount equal to the greater of actual damages or $100,000 per violation, or both (73 Pa. Stat. § 2330.9(b)). The court may increase damages up to three times the actual damages in cases where a violation has occurred with sufficient frequency to constitute a pattern of behavior (73 Pa. Stat. § 2330.9(c)). Plaintiffs may also recover fees and costs (73 Pa. Stat. § 2330.9(d)). With respect to a violation of the provision of the Act prohibiting access or use of an authorized user's modem Internet service for the purpose of causing damage to the authorized user's computer or of causing an authorized user to incur financial charges for a service that is not authorized by an authorized user (73 Pa. Stat. § 2330.4(1)(ii)), a communications provider that incurs costs for origination, transport, or termination of a call triggered by the use of a customer's modem in violation of the act may bring an action to recover the charges the provider is obligated to pay another carrier or information service provider as a result of the violation, costs of handling customer complaints with respect to amounts billed for calls, costs and reasonable attorney fees, and injunctive relief (73 Pa. Stat. § 2330.9(e)).

2. Identity Theft

Pennsylvania's identity theft law is 18 Pa. Cons. Stat. § 4120. Under the law, a plaintiff is entitled to actual damages arising from the identity theft – including loss of money, reputation or property, whether real or personal – as well as reasonable attorneys' fees and court costs (42 Pa. Cons. Stat. § 8315). In the court's discretion, the plaintiff may recover treble damages.

A person can be civilly liable for identity theft if the person possesses or uses through any means identifying information of another person without the consent of that person to further an unlawful purpose (18 Pa. Cons. Stat. § 4120(a)). For further detail, see Section I.H.

3. Invasion of Privacy

While invasion of privacy is primarily governed by Pennsylvania common law precedents, there is one statute providing for an invasion of privacy offense under specified circumstances. The law provides that a person commits the offense of invasion of privacy if he, for the purpose of arousing or gratifying the sexual desire of any person, knowingly views, photographs, videotapes, films, or otherwise records another person without that person's knowledge while the person is in a state of full or partial nudity in a place where the person has a reasonable expectation of privacy (18 Pa. Cons. Stat. § 7507.1(a)(1)). A person also commits an invasion of privacy if he knowingly views, photographs, videotapes, films, or otherwise records the intimate parts of another person without the person's knowledge and consent

and the person does not intend for the intimate parts to be visible by normal public observation (18 Pa. Cons. Stat. § 7507.1(a)(2)). A person who transports or transmits an image captured above also is guilty of a violation (18 Pa. Cons. Stat. § 7507.1(a)(3)). Exceptions are provided for law enforcement officials during a lawful criminal investigation and for law enforcement and corrections personnel for security purposes or during an investigation of alleged misconduct by a person in custody (18 Pa. Cons. Stat. § 7507.1(d)).

Separate violations occur for each victim of an offense under the same or similar circumstances pursuant to one scheme or course of conduct at the same or different times, or if a person is a victim on more than one occasion during a separate course of conduct, either individually or otherwise (18 Pa. Cons. Stat. § 7507.1 (a.1)).

Invasion of privacy is a misdemeanor in the third degree or a misdemeanor in the second degree if there is more than one violation (18 Pa. Cons. Stat. § 7507.1(b)). A prosecution for invasion of privacy must be brought within two years of the date of the offense or, if the victim did not know at the time that an offense occurred, within three years of the date the victim learned of the offense (18 Pa. Cons. Stat. § 7507.1(c)).

4. Other Causes of Action

Any person whose wire, electronic, or oral communication has been intercepted in violation of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.) has a civil cause of action against the person violating WESCA provisions. The 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. In addition, the person may recover punitive damages and reasonable attorney fees and other reasonably incurred litigation costs. The Commonwealth of Pennsylvania and its officers, officials, and employees do not have sovereign immunity with respect to an action brought under this provision (18 Pa. Cons. Stat. § 5725).

With respect to provisions of WESCA prohibiting an electronic communication service from knowingly divulging the contents of an electronic communication in the electronic storage of the service (see Section I.D.7.), persons aggrieved by a violation may bring a civil cause of action. Appropriate relief includes preliminary or other equitable or declaratory relief as appropriate, damages, and reasonable attorney fees and other reasonably incurred litigation costs. Damages may equal actual damages plus any profits made by the violator, but must be at least $1,000 (18 Pa. Cons. Stat. § 5747).

A person who has been aggrieved by a violation of provisions governing the dissemination of criminal history records (see Section I.D.5.) may bring an action for damages and may recover actual and real damages of not less than $100 for each violation and reasonable litigation costs and attorney fees. Willful violations are subject to exemplary and punitive damages of not less than $1,000 nor more than $10,000 (18 Pa. Cons. Stat. § 9183(b)).

A person whose HIV-related information has been disclosed in violation of the Confidentiality of HIV-Related Information Act (see Section I.D.9.) may bring a private cause of action to recover compensatory damages (35 Pa. Stat. § 7610).

H. Criminal Liability

The district attorneys of the several counties, as well as the Attorney General, have the authority to investigate and to institute criminal proceedings for violations of provisions regarding the confidentiality of social security numbers (see Section I.D.10.) (74 Pa. Stat. § 202).

A person who knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding use of personal information submitted by members of the public commits a deceptive or fraudulent business practice (18 Pa. Cons. Stat. § 4107(a)(10)). The violation is considered a summary offense, and violators are subject to a fine of not less than $50 nor more than $500 (18 Pa. Cons. Stat. § 4107 (a.1)(4); see Section I.H.). The district attorneys of the several counties, as well as the Attorney General, have the authority to investigate and to institute criminal proceedings for violations of the provisions described above (18 Pa. Cons. Stat. § 4107 (a.2)). In addition, financial institutions subject to the federal Gramm-Leach-

Bliley Act (GLBA) and entities covered under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Fair Credit Reporting Act are not subject to these provisions.

The district attorneys of the several counties, as well as the Attorney General, have the authority to investigate and to institute criminal proceedings for violations of the Consumer Protection Against Computer Spyware Act (see Section I.D.2.) (73 Pa. Stat. § 2330.7). A violation of specified portions of the law constitutes a second-degree felony subject to imprisonment of not more than 10 years, a fine of not more than $25,000, or both (73 Pa. Stat. § 2330.8).

Pennsylvania's identity theft law is 18 Pa. Cons. Stat. § 4120 (see Section I.G.2.). A person commits the offense of identity theft if the person possesses or uses through any means identifying information of another person without the consent of that person to further an unlawful purpose (18 Pa. Cons. Stat. § 4120(a)). Each time a person uses identifying information as described above constitutes a separate offense, but total values of offenses pursuant to one scheme, whether from the same victim or several victims, may be aggregated in determining the grade of the offense (18 Pa. Cons. Stat. § 4120(b)).

Offenses are graded as follows:

- if the total value involved is less than $2,000, a first-degree misdemeanor;
- if the total value involved is $2,000 or more, a third-degree felony;
- if the offense is committed as part of a criminal conspiracy, a third-degree felony, regardless of the amount involved; and
- if the offense is a third or subsequent offense, a second-degree felony, regardless of the amount involved (18 Pa. Cons. Stat. § 4120(c)(1)).

If a victim of identity theft is under age 18, age 60 or older, or a care-dependent person, the degrees described above are enhanced by one grade (18 Pa. Cons. Stat. § 4120(c)(2)). The Attorney General has the authority to investigate and prosecute identity theft offenses if the offense occurs in more than one county or in a different state (18 Pa. Cons. Stat. § 4120(d)).

Invasion of privacy (see Section I.G.3.) is a misdemeanor in the third degree or a misdemeanor in the second degree if there is more than one violation (18 Pa. Cons. Stat. § 7507.1(b)). A prosecution for invasion of privacy must be brought within two years of the date of the offense or, if the victim did not know at the time that an offense occurred, within three years of the date the victim learned of the offense (18 Pa. Cons. Stat. § 7507.1(c)).

Pennsylvania's anti-hacking law makes it a felony of the third degree to intentionally access a computer or network without authorization; to access a computer or network (whether intentionally or not) with the intent to interrupt a person's normal functioning or to execute a scheme to defraud; or to intentionally and knowingly, and without authorization, distribute a password or other code about a computer or network (18 Pa. Cons. Stat. § 7611).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. Attorney General

The Pennsylvania Attorney General is responsible for the enforcement of the Breach of Personal Information Notification Act (BPINA) (73 Pa. Stat. § 2301 *et seq.*; see Section I.C.8.), laws governing the privacy of social security numbers (74 Pa. Stat. § 201 *et seq.*; see Section I.D.10.), and the Wiretapping and Electronic Surveillance Control Act (WESCA) (18 Pa. Cons. Stat. § 5701 *et seq.*; see Section I.F.). The Attorney General also enforces the state's anti-spam law (Unsolicited Telecommunication Advertising Act) (73 Pa. Stat. § 2250.1 *et seq.*).

B. Other Regulators

The Department of Labor and Industry's Bureau of Labor Standards—now known as “Labor Law Compliance”—is responsible for the enforcement of the provisions of the Personnel Files Act (see Section I.E.6.; 43 Pa. Stat. § 1324).

The Public Utility Commission administers and enforces requirements related to driver history records and criminal history records relevant to drivers of vehicles required to be obtained by common or contract carriers (see Section I.D.5. and Section I.D.6.).

The Pennsylvania Insurance Department is responsible for enforcing requirements related to improper disclosures of nonpublic financial information and nonpublic health information by insurers licensed under Pennsylvania law (see Section I.E.7.).

C. SANCTIONS & FINES

Violations of the Breach of Personal Information Notification Act (BPINA) are deemed to be unfair or deceptive trade practices in violation of the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 201-1 *et seq.*). The Attorney General has the exclusive authority to bring an action under this law (73 Pa. Stat. § 2308). BPINA does not establish a private cause of action for violations.

To the extent that a person is engaged in, or about to be engaged in, activity that constitutes or will constitute a felony violation of the Wiretapping and Electronic Surveillance Control Act (WESCA) (see Section I.F.), the Attorney General may initiate an action in the Commonwealth Court to enjoin the violation (18 Pa. Cons. Stat. § 5728).

Actions violating provisions requiring persons, private entities, and state agencies to protect the confidentiality of social security numbers (see Section I.D.10.) are considered summary offenses subject to fines, as follows: not less than $50 nor more than $500 for a first offense, and for second and subsequent offenses, a fine of not less than $500 nor more than $5,000 (74 Pa. Stat. § 201(g)).

A violation of the Telephone Subscriber Directory Express Consent Act (see Section I.E.10.) is deemed to be an unfair or deceptive act or practice. The Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for violations (73 Pa. Stat. § 2407).

Violations of the anti-spam law (see Section I.E.1.) constitute violations of the Unfair Trade Practices and Consumer Protection Law, and the Attorney General may take action to enforce the law subject to administrative law and procedure requirements concerning notice, hearing, and the right of appeal (73 Pa. Stat. § 2250.5).

Any person who violates provisions of the criminal code governing the dissemination of criminal history information (see Section I.D.5.) is subject to being denied access to criminal records information, civil penalties, or in the case of an agency employee committing a violation, administrative discipline (18 Pa. Cons. Stat. § 9181). The Attorney General or any other individual or agency may institute an action to enjoin a criminal justice agency, noncriminal justice agency or organization, or individual violating these provisions or to compel the agency, organization, or individual to comply with the provisions of the law (18 Pa. Cons. Stat. § 9183(a)). A private cause of action also is available (see Section I.G.4.).

A violation of provisions of the Pennsylvania Code concerning disclosures of nonpublic financial or health information by insurers licensed in Pennsylvania (see Section I.E.7.) is considered to be an unfair method of competition and an unfair or deceptive act or practice and is subject to remedies under the Unfair Insurance Practices Act (40 Pa. Stat. § 1171.1 *et seq.*). Such remedies include issuance of a cease-and-desist order and potential suspension or revocation of license (40 Pa. Stat. § 1171.9); an action for injunctive relief on failure to comply with such a cease-and-desist order (40 Pa. Stat. § 1171.10); and civil penalties of not more than $5,000 for each knowing violation, not to exceed $50,000 for any six-month period, not more than $1,000 for a non-knowing violation, not to exceed $10,000 for any six-month period, and not more than $10,000 for violation of a cease-and-desist order (40 Pa. Stat. § 1171.11).

The Department of Health or the Insurance Department, as appropriate, may impose a civil penalty of up to $5,000 for any violation of provisions governing the responsibility of managed care plans (including HMOs) and utilization review entities to protect the confidentiality of enrollee records and restricting disclosure of such records (see Section I.D.9.).

Violations of the Telemarketer Registration Act, including the do-not-call provisions of the Act (see Section I.D.1.), are considered violations of the Unfair Trade Practices and Consumer Protection Law

(73 Pa. Stat. § 201-1 *et seq.*), and the Attorney General may seek revocation of a telemarketer's registration on a second or subsequent violation (73 Pa. Stat. § 2246). Consumers, the Attorney General, or any district attorney may pursue remedies under the Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 2247).

D. Representative Enforcement Actions

On Aug. 9, 2017, the Attorney General announced that he had reached a settlement, along with counterparts in 32 other states, with Nationwide Mutual Insurance Company with respect to a data breach from 2012 that resulted in the loss of information of 1.2 million people, including 36,000 Pennsylvanians. Under the settlement, Nationwide agreed to pay $5.5 million, $236,000 of which was earmarked for Pennsylvania. Nationwide also agreed to update its security procedures and to undertake specific actions to improve its data handling. For additional details, see the Attorney General's press release.

On Dec. 15, 2017, the Attorney General announced a $50,000 settlement with Sperian Energy Corp, a retail energy supplier that violated Pennsylvania's Do-Not-Call Law (73 Pa. Stat. § 2241 *et seq.*). According to a press release, the Office of Attorney General's Bureau of Consumer Protection investigation revealed that Sperian and its telemarketers called Pennsylvania residents whose telephone numbers were registered on the Pennsylvania "Do-Not-Call" List.

E. State Resources

Information on the do-not-call list (see Section I.E.1.) is available on the Attorney General's website. The AG also has resources regarding identity theft, and additional information on consumer protection, including complaints on unfair or deceptive trade practices, is available from the AG's Bureau of Consumer Protection.

III. RISK ENVIRONMENT

As of October 2017, there has been virtually no successful data breach litigation in a Pennsylvania state court, and the state Attorney General has not been an aggressive data security or privacy enforcer. Pennsylvania's robust "economic loss doctrine" is a formidable obstacle against negligence actions arising out of data breach, and its consumer protection law's "justifiable reliance" requirement has frustrated class certification in a number of cases. Breach of contract, express or implied, has also thus far been a dry well for plaintiffs' counsel in data breach cases. However, at least one matter currently on appeal in the Pennsylvania Supreme Court, and refinements to currently vague jurisprudence, could change some of that.

A. Negligence

1. Economic Loss Doctrine

In a standard-setting January 2017 opinion, the Pennsylvania Superior Court—one of the Commonwealth's two intermediate courts of appeal—agreed with the trial court that a putative class of employees could not proceed with a suit alleging that their employer was negligent when its system was breached and the employees' personal data was stolen. *Dittman v. UPMC*, 154 A.3d 318 (Pa. Super. 2017). The court first held that employers have no generally applicable common law duty to safeguard their employees' information and data (see supra, Section III.A.2.). Next, the court held that Pennsylvania's economic loss doctrine, which states that "no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage," *id*. at 325, barred the plaintiffs' negligence claims, because plaintiffs claimed only economic damage.

The Superior Court's view of economic loss in negligence actions arising from data breaches is shared by a variety of other courts applying Pennsylvania law. In *Longenecker-Wells v. Benecard Servs.*, 658 F. App'x 659, 661 (3d Cir. 2016), the Third Circuit relied on the economic loss doctrine to uphold the dismissal of a putative class action claiming that a prescription benefit administration services company was liable to its customers and employees because of a breach of its computer system. The

Eastern District of Pennsylvania came to a similar conclusion in *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 673 (E.D. Pa. 2015).

That said, there is some confusion among Pennsylvania courts surrounding the economic loss doctrine, particularly around whether the existence of contractual privity between the parties has any effect on its applicability. *Cf. Bilt-Rite Contractors, Inc. v. The Architectural Studio*, 581 Pa. 454, 866 A.2d 270 (Pa. 2005). On September 12, 2017, the Pennsylvania Supreme Court agreed to take up the Dittman case, to address two questions, including: "Does the economic loss doctrine permit recovery for purely pecuniary damages which result from the breach of an independent legal duty arising under common law, as opposed to the breach of a contractual duty?" *Dittman v. UPMC*, No. 149 WAL 2017, 2017 BL 319648, at *1 (Sep. 12, 2017). How the Supreme Court decides in the *Dittman* appeal has the potential to profoundly affect the shape of data breach litigation in Pennsylvania: if the court holds that the economic loss doctrine is no bar to tort causes of action in which there is no contract and the damages are purely economic, it may open the door to a wave of lawsuits that would otherwise have been unsuccessful.

2. Duty of Care

As noted above, the *Dittman* case, in addition to its economic loss holding, held that the employer had no common-law duty of care to protect its employees' information. The court applied a five-factor test to determine whether such a duty existed; key among the factors it considered was "the nature of the risk imposed and foreseeability of the harm incurred." The fact that the data breach had been caused by a third party was dispositive, because "[i]t is well established that a defendant does not have a duty to guard against the criminal acts of superseding third-parties unless he realized, or should have realized, the likelihood of such a situation." 154 A.3d 318, 323. Given that there was no reason to believe a data breach was likely, the court held that no duty of care applied.

This holding should also give potential defendants in Pennsylvania data breach litigation a measure of comfort. However, as with the economic loss doctrine, the underlying jurisprudence may soon be in flux. First, the court's reasoning in *Dittman* will not necessarily apply in every data breach case, because the reasoning in that case turned in large part on the fact that there was no particular reason to expect the breach at issue. In many cases, arguably, the defendant should have been on notice of a serious risk of breach (as, for example, where a well-known vulnerability goes unpatched), making *Dittman* potentially inapposite. And second, the Pennsylvania Supreme Court has also agreed to examine this question on appeal: "Does an employer have a legal duty to use reasonable care to safeguard sensitive personal information of its employees when the employer chooses to store such information on an internet accessible computer system?" Depending on the outcome of that appeal, employers and other holders of sensitive information may find that the do have a duty in tort to safeguard that data.

B. BREACH OF CONTRACT

Thus far, claims for breach of implied contract arising out of data breaches have been similarly unsuccessful in Pennsylvania. Courts applying Pennsylvania law have generally held that the mere fact that a party collects sensitive information from others is not enough, by itself, to imply a contractual duty on that party to protect that data from breaches. See, e.g., *Enslin v. Coca-Cola Co.*, No. 2:14-cv-06476, 2017 BL 107483, at *13 (E.D. Pa. Mar. 31, 2017); *Longenecker-Wells v. Benecard Servs.*, 658 F. App'x 659, 662; *Dittman v. UPMC*, 154 A.3d 318, 326 (Pa. Super. Ct. 2017).

That defense is not necessarily ironclad in data breach case either, however. For example, Pennsylvania courts recognize, at least in dicta, that an employee handbook can be—but is not necessarily—contractually binding; whether a given handbook does so is a highly fact-specific analysis. See, e.g., *Morosetti v. La. Land & Expl. Co.*, 564 A.2d 151, 152 (Pa. 1989); *Bauer v. Pottsville Area Emergency Med. Servs., Inc.*, 758 A.2d 1265, 1269 (Pa. Super. Ct. 2000). As a result, depending on the facts of a given case, it is quite possible that a defendant may be found to have breached a contractual duty to protect data that it collects from others.

C. Unfair Trade Practices and Consumer Protection Law

While Pennsylvania's Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. § 201-1 *et seq.*) ("UTPCPL") may provide another cause of action for consumers who, in connection with a purchase, provided companies with personal data which was subsequently breached, this avenue has been problematic for plaintiffs seeking to bring class actions. After a series of arguably inconsistent opinions on this point, the Superior Court held in January 2015 that a private plaintiff suing under the UTPCPL must prove "justifiable reliance" on the defendant's alleged misleading or confusing conduct – i.e., that not only was it justifiable to rely on the conduct at issue, the particular plaintiff actually did so. *Kern v. Lehigh Valley Hosp.*, 2015 PA Super 19, 108 A.3d 1281, 1287 (Pa. Super. 2015). This requirement makes class treatment of UTPCPL claims inappropriate in most cases, because it generally cannot be established without individualized, plaintiff-by-plaintiff discovery, that each putative class member actually did rely on the conduct. This principle led to denial of class certification in a 2016 Pennsylvania data breach case, *Baum v. Keystone Mercy Health Plan*, 145 A.3d 793 (Pa. Super. Ct. 2016). Nonetheless, plaintiffs still raise the UTPCPL in putative class actions arising out of data breaches. See, e.g., complaint in *Mann v. Equifax*, No. 2:17-cv-04100 (E.D. Pa. Sept. 13, 2017).

D. State Enforcement

Pennsylvania's Attorney General is traditionally not heavily involved in data breach and privacy enforcement. Over the past several years, Pennsylvania Attorneys General have signed on to a variety of data breach and privacy settlements, including the Lenovo settlement in September 2017 (press release), a settlement with Nationwide Mutual Insurance Co. in August 2017 (press release), the Target settlement in May 2017 (press release), the Zappos settlement in January 2015 (press release), and the Google settlement in November 2013 (press release). Each of those matters, however, involved a large number of state Attorneys General banding together to settle with a single defendant, and were likely driven by the enforcement authorities in other states. As of this writing, with the exception of a $50,000 December 2017 settlement with Sperian Energy Corp. over alleged violations of Pennsylvania's do-not-call law (press release), Pennsylvania's Attorney General has not publicly driven a data security or privacy enforcement action. That may change, however. On September 8, 2017, Attorney General Josh Shapiro announced that he had opened an investigation into the massive Equifax data breach. For additional details, see the Attorney General's press release.

E. Cybersecurity Guidance from State Agencies

Generally, Pennsylvania's state government cybersecurity and privacy guidance is not well-developed. However, at least two agencies have offered some direction for the entities they regulate.

1. Pennsylvania Public Utility Commission

Pennsylvania's vital energy industry is regulated in part by the Pennsylvania Public Utility Commission. That agency has issued modest guidance in the form of a pamphlet titled "Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities." The guidance contained in that pamphlet includes tips like "focus on human capital" to avoid risks associated with employee missteps, rather than thinking of cybersecurity as exclusively an issue to be addressed via technology; "use an assessment tool" such as the U.S. Department of Homeland Security Cybersecurity Evaluation Tool, which can guide users through a step-by-step process to assess their cybersecurity readiness; and focus on managing vendors and contractors, who can be key points of weakness if not appropriately controlled.

2. Pennsylvania Department of Banking and Securities

The state Department of Banking and Securities has created a "cybersecurity task force " and issues a quarterly newsletter focused on compliance. The task force and newsletter highlight various cybersecurity resources developed by such standard-bearers as NIST, FFIEC, FDIC, Conference of State Banking Supervisors, FTC, FCC, FINTRA, NSAA, and the SEC.

IV. EMERGING ISSUES AND OUTLOOK

A. RECENT LEGISLATION

1. Fantasy Contests & Interactive Gaming

On Oct. 30, 2017, Pennsylvania Governor Tom Wolf signed legislation (2017 Pa. Laws Act No. 42) pertaining to fantasy contests and online gaming. Among other things, the legislation provides that certain nonpublic personal information provided by an applicant for a fantasy contest license—such as "home addresses, telephone numbers and other personal contact information, social security numbers, educational records, memberships, medical records, tax returns and declarations, actual or proposed compensation, financial account records, creditworthiness or financial condition relating to an applicant or licensee"—shall remain confidential and withheld from public disclosure. See 4 Pa. Cons. Stat. § 314 (effective 4/28/2018). It also requires the establishment of "data security standards to govern age, identity and location verification of persons engaged in interactive gaming activity," 4 Pa. Cons. Stat. § 13B02(a)(14), and it requires each interactive gaming certificate holder to:

- adopt data security standards to verify the age, identity and location of persons engaged in interactive gaming and prevent unauthorized access by any person whose age, identity and location have not been verified or whose age, identity and location cannot be verified in accordance with regulations adopted by the board, 4 Pa. Cons. Stat. § 13B02(a)(15)(vii); and
- adopt standards to protect the privacy and security of registered players engaged in interactive gaming, 4 Pa. Cons. Stat. § 13B02(a)(15)(viii).

Similar data security provisions apply to slot machine licensees. 4 Pa. Cons. Stat. § 13B13(a)(1).

2. Electronic Surveillance

On July 7, 2017, Pennsylvania Governor Tom Wolf approved legislation (2017 Pa. Laws Act No. 22) amending Titles 18 (Crimes and Offenses) and 42 (Judiciary and Judicial Procedure) of the Pennsylvania Consolidated Statutes, in wiretapping and electronic surveillance, further providing for definitions, for exceptions to prohibition of interception and disclosure of communications, for exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and for expiration of chapter; and providing for recordings by law enforcement officers.

B. PROPOSED LEGISLATION

1. Data Breach Notification

SB 308, introduced Feb. 15, 2017, would amend the Breach of Personal Information Notification Act (BPINA) to require state agencies to notify affected individuals of a breach within 7 days. It would also require the Attorney General to be made aware of the breach, and for state agencies to notify the Office of Administration within 3 days following the breach. The bill also calls for the use of encryption by state employees and contractors.

HB 1548, introduced June 16, 2017, would amend BPINA by:

- updating the definition of personally identifiable information;
- revising requirements for state agencies, the Judiciary and the Legislature to notify affected individuals and supervisory and law enforcement officials in the event of a breach of personally identifiable information, and requiring businesses doing business in the Commonwealth to notify affected individuals within 14 days of the detection of the breach;
- adding protections and remedies for residents of the Commonwealth in the event of a data breach; and
- assigning responsibilities for developing policies to reduce the risk of future data breaches.

HB 1846, introduced Oct. 13, 2017, would amend BPINA by adding definitions relating to data breach notification, amending provisions relating to breach notification and notice exemption, and further providing for civil relief. The proposal was removed from the table on Jan. 2, 2018.

HB 33 offers yet another amendment to BPINA, but no action has been taken since its introduction Jan. 23, 2017. It would expand the definition of “personal Information” to bring Pennsylvania in line with how the federal government and some other states define personal information.

HB 848, introduced March 13, 2017, would require state agencies and municipalities to provide notice of data breaches involving personal information within one week. Under current law, such notice is required to be made “without necessary delay.”

2. Student Data Privacy

HB 1345, introduced May 5, 2017, would create a new chapter of Title 24 (Education) of the Pennsylvania Consolidated Statutes, providing for student data privacy and protection and imposing duties on the Department of Education.

3. Credit Reporting Agency Act Amendment

HB 1879, introduced Oct. 24, 2017, would amend the Credit Reporting Agency Act by further providing for definitions and for fees, and by providing for reimbursement for security breach and for notice of security breach.

HB 1847, introduced Oct. 13, 2017, would also amend the Credit Reporting Agency Act, further providing for definitions and for fees; providing for credit monitoring and consumer reports; and prohibiting the waiver of rights; and further providing for civil relief.

4. Internet Privacy

HB 1863, introduced Oct. 13, 2017, would regulate electronic mail solicitations; protect privacy of Internet consumers; regulate use of data about Internet users; and prescribe penalties.

5. Office of Information Technology

SB 914, introduced Oct. 5, 2017, proposes the creation of the Office of Information Technology under the Office of Administration and would consolidate all of the executive branch's information technology (IT) services, funding and oversight into this single office. A related proposal, HB 1704, was introduced Aug. 16, 2017.

C. OTHER ISSUES

1. Equifax Breach

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

