1 Data Sec. & Privacy Law § 7:9 (2016)

Data Security and Privacy Law
June 2016 Update
Chapter 7. Data Privacy Statutes

Scott L. Vernick, Esquire and Amy C. Purcell, Esquire *

I. Political Climate Mandates Increasing Privacy Regulation

§ 7:9. State security breach notification measures

Westlaw Databases
BNA Computer Technology Law Report (BNA-CTLR)
Law Reviews and Other Periodicals
Data Breaches: California Legislature Advances Bill Expanding Security Breach Notification Law, 9 Comp. Tech. L. Rep. 94 (February, 2008)
Identity Theft: State AGS Urge Congress to Establish Broad Data Breach Notification Standards, 6 Comp. Tech. L. Rep. 491 (November, 2005)
Identity Theft: Six States Jump on California Bandwagon As Governors Sign Breach Notification Laws, 6 Comp. Tech. L. Rep. 259 (May, 2005)

Another area in which there has been substantial activity at the state level has been in the domain of data security breach notification. California was again a leader in this area, having enacted its own comprehensive data security breach notification in 2002. [1] California's law, often referred to as S.B. 1386, applies to any agency, person or business that conducts business in California—even if the business itself is not based in California. Pursuant to S.B. 1386, which entered into force on July 1, 2003, all agencies, persons or businesses that conduct business in California and that own or license computerized data containing personal information will be required to report breaches in the security of such data to any resident of California whose unencrypted personal information has been compromised as a result of the breach. [2]

In order to trigger the notification requirements under the law, the security breach must involve personal information, which is defined as an individuals first name or first initial and last name combined with one or more of the following pieces of data: (i) social security number; (ii) drivers license number or California Identification Card number; or (iii) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individuals financial account. [3] In 2008, California amended its notification law to include medical and health insurance information. [4] Furthermore, the notification requirements will only be triggered in situations in which either the name or the additional data elements are not encrypted.

In 2013 (effective January 1, 2014), California again amended the definition of personal information to include, when unencrypted, "a username or email address, in combination with a password or security question and answer that would permit access to an online account." [5]

Where an agency, person or business is processing such personal information and suffers a breach of the security of its systems, it must notify the affected customers in "the most expedient time possible and without unreasonable delay." [6] Under an amendment (effective January 1, 2012), if an agency, person or business provides notice to more than 500 California residents in connection with a single breach, the agency, person or business must send a copy of that notification to the Attorney General. [7] Significantly, the law defines a breach of security broadly as an "unauthorized acquisition of computerized data that

compromises the security, confidentiality, or integrity of personal information maintained by the agency, person or business." [8]

Individuals or entities required to provide such notice may do so in writing or electronically. However, all electronic notices must be in compliance with the federal Electronic Signatures in Global and National Commerce Act of 2000. Beginning on January 1, 2011, there are specific guidelines that must be followed when drafting a notice. [9] For example, notices must contain a "list of the types of personal information that were or are reasonably believed to have been the subject of a breach" and a "general description of the breach incident." [10] Notwithstanding the foregoing, in instances where (i) the cost of providing the requisite notice would exceed $250,000, (ii) the number of people to be notified exceeds 500,000, or (iii) there is no sufficient contact information available, the affected individual or entity may provide substitute notice, which would consist of providing all of the following (i) e-mail notice if e-mail addresses are available; (ii) Web site notice provided there is a Web site that can be used to post such notice; and (iii) notification to major statewide media. [11]

After a series of high-profile data security breaches in the early part of 2005, numerous states rushed to follow suit, enacting their own breach notification measures, the bulk of which are modeled closely after California's measure. See § 7:67 for a table of the measures undertaken to date at the state level in this regard. [12] Certain states, however, have enacted notification statutes that expand the requirements set forth in the California statute. For example, the notification statute enacted by Idaho in 2010, requires a city, county, or state agency to notify the state attorney general of a breach of personal data within 24 hours of discovering the breach. [13]

In fact, to date, Alabama, New Mexico and South Dakota are the only states that do not have a security breach notification statute. [14] One of the most recent states to enact a notification statute was Mississippi. Mississippi House Bill 583, which became effective on July 1, 2011, requires notice of a security breach to affected residents only (not government regulators or credit reporting agencies). [15] House Bill 583 uses the "classic" definition of personal information (before California's amendment to include medical and health insurance information). [16] Unlike California, however, Mississippi's law contains a "risk of harm threshold" and requires notice if "after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals." [17]

In 2010, Virginia enacted a law that requires governmental entities, or other organizations "supported wholly or principally by public funds" to provide notice of breaches of a person's medical information. [18] The law defines medical information to include the first name or initial and last name in combination with any of the following: (1) information regarding a person's medical history, mental or physical condition, medical treatment or diagnosis; or (2) a person's health insurance policy number, subscriber identification number, any unique identifier or any information regarding a person's health insurance application and claims history. [19] Under the law, a breach means "unauthorized access and acquisition of unencrypted or unredacted computerized data." [20] A breach also includes encrypted data if the encryption key is also acquired. [21] The law requires that, in the event of a breach, the entity must notify affected Virginia residents, as well as the Virginia Attorney General. [22] In 2010, New Hampshire passed legislation that requires health care providers to (1) obtain an authorization from individuals before using or disclosing their protected health information ('PHI') for marketing, and (2) provide an opportunity for individuals to choose not to receive fundraising communications that involve their PHI. [23] In 2012, Vermont amended its data breach notification statute to require entities to notify consumers no later than 45 days after discovery of the incident and to include in the notice the approximate date of the incident, if known. [24]

States have also began to require "data collectors" that accept payment cards to comply with the Payment Card Industry Data Security Standard (PCI DSS). [25] Beginning on January 1, 2010, Nevada became the

first state to require complete compliance with the PCI DSS.[26] The Nevada law applies to government agencies and businesses that accept payment cards and conduct business in the state.[27] The Nevada law also requires data collectors who do not accept payment cards to encrypt all personal information when transferring it "outside of the secure system of the data collector" and when moving any data storage device that contains personal information "beyond the logical or physical controls of the data collector."[28] The Nevada law, however, contains a safe harbor provision.[29] A data collector is not liable for damages as a result of a security breach if: (1) "the data collector is in compliance with the PCI DSS or encryption requirements"; or (2) "the security breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees, or agents."[30]

Similarly, Washington passed House Bill 1149 (effective July 1, 2010), which incorporates the PCI DSS in an effort to help financial institutions recoup costs associated with data breaches.[31] Washington's bill states that businesses that process more than six million debit or credit cards transactions a year may be found liable for failing to exercise "reasonable care" by encrypting personal information.[32] The bill also holds vendors responsible for damages if a breach occurs as a result of a "defect" in the vendor's software.[33] However, the bill provides a safe harbor provision if an entity's compliance with the PCI DSS was validated by a security assessment within one year before the breach.[34] Under House Bill 1149, financial institutions may seek reimbursement from businesses or vendors for the costs associated with reissuing cards to individual's affected by a breach.[35]

In addition to its breach notification statute, effective March 1, 2010, Massachusetts enacted information security regulations, titled "Standards for Protection of Personal Information of Residents of the Commonwealth."[36] These regulations apply to any person or business that owns or licenses personal information of residents of Massachusetts. The regulations require entities to develop, implement and maintain a written "comprehensive information security program" based upon an entity's size, nature of business, types of records it maintains and the risk of identity theft posed by the entity's operations. The regulations also mandate certain safeguards that an entity must include in its information security program. The regulations also require entities to follow certain procedures when selecting and retaining service providers that will deal with personal information,[37] such as requiring specific language in third-party contracts obligating vendors to use reasonable measures to protect personal information.[38] The Massachusetts regulations apply to all businesses that store personal information pertaining to state residents, regardless of where the businesses are located.[39]

New Jersey also passed legislation related to the destruction of data stored on digital copiers and scanners. The New Jersey legislation requires that "a person destroy, or arrange for the destruction of, all records stored on a digital copy machine, which is no longer to be retained by that person, by erasing or otherwise modifying those records to make the records unreadable, undecipherable, or nonreconstructable through generally available means."[40] The bill states that both the lessor and the lessee of a digital copier or scanner are responsible for the destruction of the data. The bill also requires manufacturers of digital copiers and scanners to include instructions with these machines explaining how to destroy the data.[41]

* Scott L. Vernick is a partner, chair of the Privacy and Data Security Practice and member of the Executive Committee at the national law firm of Fox Rothschild LLP, resident in its Philadelphia office. For nine consecutive years, Chambers USA has ranked him as a leading litigation attorney in Pennsylvania. Mr. Vernick's diverse national trial practice focuses on technology, intellectual property, health care, privacy and data security for *Fortune* 500 clients, including First Data

Corporation, GlaxoSmithKline and Merck & Co., Inc. He represents clients in state and federal courts, as well as in arbitration forums, in commercial disputes regarding licensing and technology transfer agreements; intellectual property, trade secrets, restrictive covenants and unfair competition; software and hardware technology service agreements; merchant processing and electronic payments; mergers, acquisitions and corporate changes-of-control; government contracting and procurement; and commercial lending, FCRA, FDCPA and TILA. Over the past decade, Mr. Vernick has developed a particular fluency in the rapidly evolving field of privacy and data security. He routinely counsels multinational and mid-sized businesses on how to mitigate risk and overcome the challenges posed by the current state and federal enforcement environment. Mr. Vernick spearheaded the creation of the firm's Data Breach 411 iPhone app, which provides immediate access to state data breach notification statutes, as well as other pertinent resources. As a recognized authority on privacy and data security, he is routinely quoted on these issues in outlets including *Forbes, The Economist, The Guardian, The Wall Street Journal, The Washington Post,* Crain's *New York Business, The Huffington Post, USA Today* and *The New York Times,* and has also appeared on "The O'Reilly Factor," "The Willis Report," NBC Philadelphia, NPR and Fox News. He earned his J.D., cum laude, from Georgetown University in 1987 and his B.A. from Trinity College in 1983. Mr. Vernick can be reached at 215.299.2860 or svernick@foxrothschild.com. Amy C. Purcell is a partner at the national law firm of Fox Rothschild LLP. Resident in the Philadelphia office, she is a trusted source on all aspects of commercial and business-related litigation, including contractual disputes, electronic data security/privacy rights, alternative dispute resolution, misappropriation of trade secrets, restrictive covenants, unfair competition, false advertising, merchant processing and electronic payments. In addition to representing clients in state and federal courts and in arbitration forums, Ms. Purcell routinely represents clients in privacy and electronic data security matters on a national level. She handles data security investigations and remediation efforts, as well as claims and lawsuits alleging violations of privacy. In her role, Ms. Purcell assists clients in taking the necessary steps to protect themselves against data breaches, providing guidance on the creation and enforcement of company-wide policies and programs to ensure compliance with state and federal laws, and advising clients on how to respond to data security breaches. She was instrumental in the creation of the firm's Data Breach 411 iPhone app—which offers quick access to data breach notification rules from state to state—and is a frequent contributor to the firm's Privacy Compliance & Data Security blog (http://dataprivacy.foxrothschild.com) and a co-editor of the Tech in the Workplace blog (http://techintheworkplace.foxrothschild.com/). Ms. Purcell earned her J.D. from Cornell University and her B.A. from Susquehanna University. Ms. Purcell can be reached at 215.299.2798 or apurcell@foxrothschild.com.

1 Cal. Civ. Code §§ 1798.29, 1798.82 to 1798.84.

2 Cal. Civ. Code § 1798.29(a).

3 Cal. Civ. Civil Code § 1798.29(e).

4 Kevin D. Lyles and Jeffrey M. Rawitz, California Expands Security Breach Notification Law To Include Medical And Health Insurance Information, mondaq, Sept. 30, 2008, available at http://www.mondaq.com/unitedstates/article.asp?articleid=66994 (last visited Feb. 28, 2014).

5 Joseph Duffy, et al., New California law protects online account information, Association of Corporate Counsel, Oct. 11, 2013, available at http://www.lexology.com/library/detail.aspx?g=24fc38db-e729-458f-8983-1a13d7580b04 (last visited Feb. 28, 2014).

6 Cal. Civ. Civil Code § 1798.29(a).

7 Cal. Civ. Code §§ 1798.29(e) and 1798.82(f); Senate Bill No. 24.

8 Cal. Civ. Civil Code § 1798.29(d).

9 Cal. Civ. Code §§ 1798.29(d) and 1798.82(d); Senate Bill No. 24.

10 Cal. Civ. Code §§ 1798.29(d) and 1798.82(d); Senate Bill No. 24.

11 Cal. Civ. Civil Code § 1798.29(g).

12 See also National Conference of State Legislatures, 2005 Breach of Information Security Legislation, available at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm (last visited Dec. 18, 2005).

13 See Idaho Code §§ 28-51-105; see also http://www.steptoe.com/publications-6821.html.

14 See *Security Breach Notification Laws,* National Conference of State Legislatures, Jan. 12, 2015, available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

15 H.B. 583, Regular Sess. (Miss. 2010) available at: http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf.

16 H.B. 583, Regular Sess. (Miss. 2010) available at: http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf.

17 H.B. 583, Regular Sess. (Miss. 2010) available at: http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf.

18 David Navetta, Virginia Adds Medical Information Breach Notice Law, Apr. 7, 2010, InformationLawGroup,

available http://www.infolawgroup.com/2010/04/articles/breach-notice/virginia-adds-medical-information-breach-notice-law/ (last visited Feb. 28, 2014); see also Breach of medical information notification (Va. Code Ann. § 32.1-127.1:05) http://leg6.state.va.us/cgi-bin/legp604.exe?101+ful +HB1039ER (last visited Feb. 28, 2014).

19 David Navetta, Virginia Adds Medical Information Breach Notice Law, Apr. 7, 2010, InformationLawGroup, available http://www.infolawgroup.com/2010/04/articles/breach-notice/virginia-adds-medical-information-breach-notice-law/ (last visited Feb. 28, 2014); see also Breach of medical information notification (Va. Code Ann. § 32.1-127.1:05) http://leg6.state.va.us/cgi-bin/legp604.exe?101+ful +HB1039ER (last visited Feb. 28, 2014).

20 Va. Code Ann. § 32.1-127.1:05.A.

21 Va. Code Ann. § 32.1-127.1:05.C.

22 Va. Code Ann. § 32.1-127.1:05.B.

23 http://www.huntonprivacyblog.com/2010/01/articles/hipaa-1/ nevada-and-new-hampshire-data-security-and-privacy-laws-take-effect/; N.H. Rev. Stat. Ann. §§ 359-C:19, 359-C:20, 359-C:21.

24 Vt. Stat. Ann. tit. 9, § 2435.

25 Nev. Rev. Stat. §§ 603A.010 et seq.

26 http://www.huntonprivacyblog.com/2010/01/articles/hipaa-1/ nevada-and-new-hampshire-data-security-and-privacy-laws-take-effect/.

27 http://www.huntonprivacyblog.com/2010/01/articles/hipaa-1/ nevada-and-new-hampshire-data-security-and-privacy-laws-take-effect/.

28 2009 Nev. S.B. 227 (NS); http://www.dlapiper.com/amended-nevada-law-mandates-encryption-compliance-with-pci-data-security-standard/.

29 2009 Nev. S.B. 227 (NS); http://www.dlapiper.com/amended-nevada-law-mandates-encryption-compliance-with-pci-data-security-standard/.

30 2009 Nev. S.B. 227 (NS); http://www.dlapiper.com/amended-nevada-law-mandates-encryption-compliance-with-pci-data-security-standard/.

31 Linda McGlasson, Does new Data Breach Law Have Teeth?, Bank InfoSecurity, April 12, 2010, at: http:// www.bankinfosecurity.com/articles.php?art_id=2403.

32 Linda McGlasson, Does new Data Breach Law Have Teeth?, Bank InfoSecurity, April 12, 2010, at: http:// www.bankinfosecurity.com/articles.php?art_id=2403.

33 Linda McGlasson, Does new Data Breach Law Have Teeth?, Bank InfoSecurity, April 12, 2010, at: http://www.bankinfosecurity.com/articles.php?art_id=2403.

34 Addition to Washington breach law imposes retailer liability in payment card breaches, Hunton & Williams LLP Blog, March 24, 2010, at: http://www.huntonprivacyblog.com/2010/03/articles/security-breach/addition-to-washington-breach-law-imposes-retailer-liability-in-payment-card-breaches/%23page=1.

35 Addition to Washington breach law imposes retailer liability in payment card breaches, Hunton & Williams LLP Blog, March 24, 2010, at: http://www.huntonprivacyblog.com/2010/03/articles/security-breach/addition-to-washington-breach-law-imposes-retailer-liability-in-payment-card-breaches/%23page=1.

36 Mass. Regs. Code tit. 201, § 17.00; http://www.huntonprivacyblog.com/2010/02/articles/massachusetts-information-security-regulations-take-effect-on-march-1-2010/#more-1526.

37 Mass. Regs. Code tit. 201, § 17.00; http://www.huntonprivacyblog.com/2010/02/articles/massachusetts-information-security-regulations-take-effect-on-march-1-2010/#more-1526.

38 Jaikumar Vijayan, Final phase of Mass. data protection law kicks in March 1, Computerworld (Jan. 25, 2012) at http://www.computerworld.com/s/article/9223709/Final_phase_of_Mass._data_protection_law_kicks_in_March_1?taxonomyId=19.

39 Jaikumar Vijayan, Final phase of Mass. data protection law kicks in March 1, Computerworld (Jan. 25, 2012) at http://www.computerworld.com/s/article/9223709/Final_phase_of_Mass._data_protection_law_kicks_in_March_1?taxonomyId=19.

40 New Jersey Assembly passes bill requiring deletion of copier data, InfoSecurity (June 1, 2012) at http://www.infosecurity-magazine.com/view/26127/new-jersey-assembly-passes-bill-requiring-deletion-of-copier-data.

41 New Jersey Assembly passes bill requiring deletion of copier data, InfoSecurity (June 1, 2012) at http://www.infosecurity-magazine.com/view/26127/new-jersey-assembly-passes-bill-requiring-deletion-of-copier-data.

End of Document

West's Idaho Code Annotated
Title 28. Commercial Transactions
Chapter 51. Identity Theft

I.C. § 28-51-105

§ 28-51-105. Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity

Currentness

(1) A city, county or state agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

When an agency becomes aware of a breach of the security of the system, it shall, within twenty-four (24) hours of such discovery, notify the office of the Idaho attorney general. Nothing contained in this section relieves a state agency's responsibility to report a security breach to the office of the chief information officer within the department of administration, pursuant to the Idaho technology authority policies.

Any governmental employee who intentionally discloses personal information not subject to disclosure otherwise allowed by law is guilty of a misdemeanor and, upon conviction thereof, shall be punished by a fine of not more than two thousand dollars ($2,000), or by imprisonment in the county jail for a period of not more than one (1) year, or both.

(2) An agency, individual or a commercial entity that maintains computerized data that includes personal information that the agency, individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

(3) Notice required by this section may be delayed if a law enforcement agency advises the agency, individual or commercial entity that the notice will impede a criminal investigation. Notice required by this section must be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency advises the agency, individual or commercial entity that notification will no longer impede the investigation.

Credits

Added by S.L. 2006, ch. 258, § 1, eff. July 1, 2006. Amended by S.L. 2010, ch. 170, § 1, eff. July 1, 2010; S.L. 2014, ch. 97, § 13, eff. July 1, 2014.

I.C. § 28-51-105, ID ST § 28-51-105

The statutes and Constitution are current through the 2016 Second Regular Session of the 63rd Idaho Legislature.

End of Document

§ 28-51-107. VIOLATIONS.

Idaho Statutes

Title 28. COMMERCIAL TRANSACTIONS

Chapter 51. IDENTITY THEFT

Current through Chapter 329 of the 2019 Regular Session

§ 28-51-107. VIOLATIONS

In any case in which an agency's, commercial entity's or individual's primary regulator has reason to believe that an agency, individual or commercial entity subject to that primary regulator's jurisdiction under section 28-51-104(6), Idaho Code, has violated section 28-51-105, Idaho Code, by failing to give notice in accordance with that section, the primary regulator may bring a civil action to enforce compliance with that section and enjoin that agency, individual or commercial entity from further violations. Any agency, individual or commercial entity that intentionally fails to give notice in accordance with section 28-51-105, Idaho Code, shall be subject to a fine of not more than twenty-five thousand dollars ($25,000) per breach of the security of the system.

Cite as Idaho Code § 28-51-107

§ 19.255.010. Disclosure, notice-Definitions-Rights, remedies.

Washington Statutes

Title 19. BUSINESS REGULATIONS-MISCELLANEOUS

Chapter 19.255. Personal information-Notice of security breaches

Current through Chapter 38, 2016 First Special Session

§ 19.255.010. Disclosure, notice-Definitions-Rights, remedies

(1) Any person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. Notice is not required if the breach of the security of the system is not reasonably likely to subject consumers to a risk of harm. The breach of secured personal information must be disclosed if the information acquired and accessed is not secured during a security breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

(2) Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(3) The notification required by this section may be delayed if the data owner or licensee contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system when the personal information is not used or subject to further unauthorized disclosure.

(5) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data

elements:

(a) Social security number;

(b) Driver's license number or Washington identification card number; or

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

(6) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(7) For purposes of this section, "secured" means encrypted in a manner that meets or exceeds the national institute of standards and technology (NIST) standard or is otherwise modified so that the personal information is rendered unreadable, unusable, or undecipherable by an unauthorized person.

(8) For purposes of this section and except under subsections (9) and (10) of this section, "notice" may be provided by one of the following methods:

(a) Written notice;

(b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec. 7001; or

(c) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) Email notice when the person or business has an email address for the subject persons;

(ii) Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one; and

(iii) Notification to major statewide media.

(9) A person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section is in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(10) A covered entity under the federal health insurance portability and accountability act of

1996, 42 U.S.C. Sec. 1320d et seq., is deemed to have complied with the requirements of this section with respect to protected health information if it has complied with section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015. Covered entities shall notify the attorney general pursuant to subsection (15) of this section in compliance with the timeliness of notification requirements of section 13402 of the federal health information technology for economic and clinical health act, Public Law 111-5 as it existed on July 24, 2015, notwithstanding the notification requirement in subsection (16) of this section.

(11) A financial institution under the authority of the office of the comptroller of the currency, the federal deposit insurance corporation, the national credit union administration, or the federal reserve system is deemed to have complied with the requirements of this section with respect to "sensitive customer information" as defined in the interagency guidelines establishing information security standards, 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2, 12 C.F.R. Part 225, Appendix F, and 12 C.F.R. Part 364, Appendix B, and 12 C.F.R. Part 748, Appendices A and B, as they existed on July 24, 2015, if the financial institution provides notice to affected consumers pursuant to the interagency guidelines and the notice complies with the customer notice provisions of the interagency guidelines establishing information security standards and the interagency guidance on response programs for unauthorized access to customer information and customer notice under 12 C.F.R. Part 364 as it existed on July 24, 2015. The entity shall notify the attorney general pursuant to subsection (15) of this section in addition to providing notice to its primary federal regulator.

(12) Any waiver of the provisions of this section is contrary to public policy, and is void and unenforceable.

(13) (a) Any consumer injured by a violation of this section may institute a civil action to recover damages.

(b) Any person or business that violates, proposes to violate, or has violated this section may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

(14) Any person or business that is required to issue notification pursuant to this section shall meet all of the following requirements:

(a) The notification must be written in plain language; and

(b) The notification must include, at a minimum, the following information:

(i) The name and contact information of the reporting person or business subject to this section;

(ii) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach; and

(iii) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information.

(15) Any person or business that is required to issue a notification pursuant to this section to more than five hundred Washington residents as a result of a single breach shall, by the time notice is provided to affected consumers, electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the attorney general. The person or business shall also provide to the attorney general the number of Washington consumers affected by the breach, or an estimate if the exact number is not known.

(16) Notification to affected consumers and to the attorney general under this section must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered, unless at the request of law enforcement as provided in subsection (3) of this section, or due to any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(17) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this section. For actions brought by the attorney general to enforce this section, the legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. For actions brought by the attorney general to enforce this section, a violation of this section is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this section may not be brought under RCW 19.86.090.

Cite as RCW 19.255.010

History. Amended by 2015 c 64, §2, eff. 7/24/2015.

2005 c 368 § 2.

Note:

Intent- 2015 c 64 : "The legislature recognizes that data breaches of personal information can compromise financial security and be costly to consumers. The legislature intends to strengthen the data breach notification requirements to better safeguard personal information, prevent identity theft, and ensure that the attorney general receives notification when breaches occur so that appropriate action may be taken to protect consumers. The legislature also intends to provide consumers whose personal information has been jeopardized due to a data breach with the information

needed to secure financial accounts and make the necessary reports in a timely manner to minimize harm from identity theft." [2015 c 64 §1.]

Similar provision: RCW 42.56.590.

PLEASE READ THE ENTIRE POLICY CAREFULLY

CLAIMS MADE AND REPORTED POLICY

THIS POLICY CONTAINS CERTAIN CLAIMS MADE AND REPORTED COVERAGES UNDER INSURING AGREEMENTS 1, 3, 4, AND 5. THEREFORE, WITH RESPECT TO THOSE COVERAGES, THE "INSURED" MUST IMMEDIATELY REPORT ANY "CLAIM" TO ALPS PROPERTY & CASUALTY INSURANCE COMPANY ("ALPS") DURING THE "POLICY PERIOD" OR DURING ANY "EXTENDED REPORTING PERIOD" (IF APPLICABLE). WITH RESPECT TO THOSE COVERAGES, NO COVERAGE EXISTS UNDER THIS POLICY FOR A "CLAIM" WHICH IS FIRST MADE AGAINST THE "INSURED" OR FIRST REPORTED TO ALPS BEFORE OR AFTER THE "POLICY PERIOD" OR ANY APPLICABLE "EXTENDED REPORTING PERIOD". IF THE "INSURED" RECEIVES NOTICE OF A "CLAIM", OR BECOMES AWARE OF ANY FACTS, EVENTS OR CIRCUMSTANCES THAT COULD REASONABLY BE EXPECTED TO BE THE BASIS OF A "CLAIM", THE "INSURED" MUST IMMEDIATELY DELIVER A WRITTEN NOTICE OF THE "CLAIM" OR THE FACTS, EVENTS OR CIRCUMSTANCES THAT COULD REASONABLY BE EXPECTED TO BE THE BASIS OF A "CLAIM" DIRECTLY TO ALPS VIA EMAIL, FACSIMILE, OR MAIL AT ANY OF THE FOLLOWING:

NOTICE OF CLAIM

Email:	*Claims@alpsnet.com*
Facsimile:	406-728-7416
Mail Address:	ALPS 111 N. Higgins, Ste. 600 P.O. Box 9169 Missoula, MT 59807-9169

If you deliver notice of a "claim" or facts, events or circumstances that may give rise to a "claim" to ALPS via email at Claims@alpsnet.com, you must then receive an email from the ALPS Account Center Portal acknowledging receipt of the notice before the notice is considered to have been received by ALPS. If you do not receive an acknowledging email from ALPS by the end of the next business day after delivering a notice to ALPS via email, then please contact ALPS at 406-728-3113 for further assistance.

LIMIT OF LIABILITY AND DEFENSE COSTS

The policy aggregate limit of liability shall be reduced and may be completely exhausted by payment of "claims expenses". Our right and duty to defend any "claim" ends when the policy aggregate limit of liability has been exhausted, and in such event, the "named insured" shall, upon notice from us, promptly assume responsibility for and take over control of defense of the "claim".

SEPARATE AND DISTINCT INSURANCE POLICY AND LIMIT OF LIABILITY

This Cyber Liability and Data Breach Response Insurance Policy is a separate insuring agreement and distinct from any other insurance policy we may issue to you. Each insurance policy we issue to you should be considered a separate and independent insuring agreement with its own separate terms, conditions and definitions. No coverage is afforded under this Policy for any "claim" that is otherwise covered under any other insurance policy we issue to you. The limits of liability provided by each separate insurance policy we issue to you shall apply only to losses under that policy and shall not be added together with the limits of liability of any other insurance policy we issue to you.

IMPORTANT NOTICE

INSURING AGREEMENTS 1., 3., 4., AND 5. SET FORTH IN SECTION I OF THIS POLICY PROVIDE COVERAGE ON A "CLAIMS MADE AND REPORTED" BASIS AND APPLY ONLY TO "CLAIMS" FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR THE EXTENDED REPORTING PERIOD, IF APPLICABLE, AND FIRST REPORTED TO US DURING THE POLICY PERIOD OR AS OTHERWISE PROVIDED IN **SECTION VII.** AMOUNTS INCURRED AS "CLAIMS EXPENSES" UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE APPLICABLE LIMIT OF LIABILITY AND ARE SUBJECT TO APPLICABLE RETENTIONS.

INSURING AGREEMENTS 2., 6., 7., 8., 9. AND 10. SET FORTH IN SECTION I OF THIS POLICY PROVIDE FIRST PARTY COVERAGE ON AN "INCIDENT DISCOVERED AND REPORTED" BASIS AND APPLY ONLY TO INCIDENTS FIRST DISCOVERED BY THE INSURED AND FIRST REPORTED TO THE UNDERWRITERS DURING THE "POLICY PERIOD".

Throughout this Policy, the words "you" and "your" refer to the "named insured(s)" shown in the "Policy Declarations" and any other person(s) or organization(s) qualifying as a "named insured" under this Policy. The words "we", "us" and "our" refer to ALPS Property & Casualty Insurance Company, a Montana stock corporation. The word insured means any person or organization qualifying as such under **SECTION III- INSURED AND INSURED ORGANIZATION.**

Various provisions in this Policy restrict coverage. Read the entire Policy carefully to determine your rights and duties and what is and is not covered. The terms, conditions, exclusions, and limits of liability set forth in this Policy apply only to the coverage provided by this Policy.

Words and phrases that appear in quotation marks have special meaning as set forth in **SECTION XXIV – DEFINITIONS.**

SECTION I – INSURING AGREEMENTS

Coverage is provided under the following insuring agreements for which a policy aggregate limit of liability is shown in the "Policy Declarations":

1. Information Security and Privacy Liability

We will pay on behalf of the insured, "damages" and "claims expenses", in excess of the "retention", which the insured shall become legally obligated to pay because of any "claim", including a "claim" for a violation of a "privacy law", first made against any insured during the "policy period" or optional "extended reporting period", if applicable, and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM** for:

A. theft, loss, or "unauthorized disclosure" of "personally identifiable information" or "third party information" that is in the care, custody or control of the "insured organization", or a third party for whose theft, loss or "unauthorized disclosure" of "personally identifiable information" or "third party information" the "insured organization" is legally liable (a third party shall include a business associate as defined by the Health Insurance Portability and Accountability Act (HIPAA)), provided such theft, loss or "unauthorized disclosure" first takes place on or after the "retroactive date" and before the end of the "policy period";

B. one or more of the following acts or incidents that directly result from a failure of "computer security" to prevent a "security breach", provided that such act or incident first takes place on or after the "retroactive date" and before the end of the "policy period":

- **i.** the alteration, corruption, destruction, deletion, or damage to data stored on "computer systems";
- **ii.** the failure to prevent transmission of "malicious code" from "computer systems" to computer or network systems that are not owned, operated or controlled by an insured; or
- **iii.** the participation by the "insured organization's" "computer systems" in a "denial of service attack" directed against a computer or network systems that are not owned, operated or controlled by an insured;

C. the "insured organization's" failure to timely disclose an incident described in paragraphs A. or B. of this section in violation of any "breach notice law"; provided such incident giving rise to the "insured organization's" obligation under a "breach notice law" must first take place on or after the "retroactive date" and before the end of the "policy period";

D. failure by the insured to comply with that part of a "privacy policy" that specifically:
   i. prohibits or restricts the "insured organization's" disclosure, sharing or selling of a person's "personally identifiable information";
   ii. requires the "insured organization" to provide access to "personally identifiable information" or to correct incomplete or inaccurate "personally identifiable information" after a request is made by a person; or
   iii. mandates procedures and requirements to prevent the loss of "personally identifiable information";

   provided the acts, errors or omissions that constitute such failure to comply with a "privacy policy" must first take place on or after the "retroactive date" and before the end of the "policy period", and the "insured organization" must, at the time of such acts, errors or omissions, have in force a "privacy policy" that addresses those subsections above that are relevant to such "claim"; or

E. failure by the insured to administer:
   i. an identity theft prevention program as required by regulations and guidelines promulgated pursuant to 15 U.S.C. §1681m(e), as amended, or
   ii. an information disposal program required by regulations and guidelines promulgated pursuant to 15 U.S.C §1681W, as amended;

   provided the acts, errors or omissions that constitute such failure must first take place on or after the "retroactive date" and before the end of the "policy period".

2. Privacy Breach Response Services

We will provide privacy breach response services to the "insured organization, in excess of the "retention", because of an incident, or a reasonably suspected incident, described in paragraphs A. or B. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**, that first takes place on or after the "retroactive date" and before the end of the "policy period" and is discovered by the insured and is reported to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM.**

Privacy breach response services means the following:

A. "computer expert services";
B. "legal services";
C. "public relations and crisis management expenses";
D. "notification services" to provide notification to:
   i. individuals who are required to be notified by the "insured organization" under the applicable "breach notice law"; or
   ii. in our discretion, individuals affected by an incident in which their "personally identifiable information" has been subject to theft, loss, or "unauthorized disclosure" in a manner which compromises the security or privacy of such individual by posing a significant risk of financial, reputational or other harm to the individual;
E. "call center services"; and
F. "breach resolution and mitigation services".

With respect to privacy breach responses services as defined above:

   i. paragraphs A.-C. of this Section 2 are subject to a monetary limit in excess of the "retention" as noted in the "Policy Declarations"; and
   ii. paragraphs D., E. and F. of this Section 2 are subject to a maximum notified individual limit and the "retention" noted in the "Policy Declarations".

Privacy Breach Response Services will be provided subject to the terms and conditions of this Policy and will be subject to the applicable "retentions" and limitations set forth in the "Policy Declarations" and shall not include any internal salary or overhead expenses of the "insured organization".

3. Regulatory Defense and Penalties

We will pay on behalf of the insured, "claims expenses" and "penalties" , in excess of the "retention", which the insured shall become legally obligated to pay because of any "claim" in the form of a "regulatory proceeding", first made against any insured during the "policy period" or the optional "extended reporting period", if applicable, and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**, for a violation of a "privacy law" and caused by an

incident described in paragraphs A., B. or C. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** that first takes place on or after the "retroactive date" and before the end of the "policy period".

4. **Website Media Content Liability**
We will pay on behalf of the insured, "damages" and "claims expenses", in excess of the "retention", which the insured becomes legally obligated to pay resulting from any "claim" first made against any insured during the "policy period" or the optional "extended reporting period", if applicable, and reported in writing to us during the "policy period", or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**, for one or more of the following acts first committed on or after the "retroactive date" and before the end of the "policy period" in the course of the "insured organization's" display of "media material" on its website or on social media web pages created and maintained by or on behalf of the "insured organization":
   A. defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related to disparagement or harm to the reputation or character of any person or organization;
   B. a violation of the rights of privacy of an individual, including false light and public disclosure of private facts;
   C. invasion of or interference with an individual's right of publicity, including commercial appropriation of name, persona, voice or likeness;
   D. plagiarism, piracy or misappropriation of ideas under implied contract;
   E. infringement of copyright;
   F. infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, slogan, service mark, service name; or
   G. improper deep-linking or framing within electronic content.

5. **PCI Fines, Expenses and Costs**
We will indemnify the insured for "PCI fines, expenses, and costs", in excess of the "retention", which the insured shall become legally obligated to pay because of a "claim" first made against any insured during the "policy period" or optional "extended reporting period", if applicable, and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**. Coverage under this insuring agreement is sub-limited to the amount set forth in the "Policy Declarations" and we have no duty to defend any "claim" or pay any "claims expenses" with respect to any "claim" under this insuring agreement.

6. **Cyber Extortion**
We will indemnify the "named insured" for "cyber extortion loss", in excess of the "retention", incurred by the "insured organization" as a direct result of an "extortion threat" first made against the "insured organization" during the "policy period" and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**. We will not pay for "cyber extortion loss" which is part of a series of related "extortion threats" that began prior to the "policy period".

7. **First Party Data Protection**
We will indemnify the "named insured" for "data protection loss", in excess of the "retention", incurred by the "insured organization" as a direct result of:
   A. alteration, corruption, destruction, deletion or damage to a "data asset", or
   B. inability to access a "data asset"
that is directly caused by a failure of "computer security" to prevent a "security breach"; provided that such "security breach" takes place on or after the "retroactive date" and before the end of the "policy period" and is reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**.

8. **First Party Network Business Interruption**
We will indemnify the "named insured" for "business interruption loss", in excess of the "retention", the "insured organization" sustains during the "period of restoration" as a direct result of the actual and necessary interruption of "computer systems" caused directly by a failure of "computer security" to prevent a "security breach"; provided such "security breach" must first take place on or after the "retroactive date" and before the end of the "policy period" and is reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**.

9. **Fraudulent Instruction**
We will indemnify the "named insured" for loss, in excess of the applicable "retention", resulting directly from an insured having transferred, paid, or delivered any "money" or "securities" as a direct result of "fraudulent instructions", provided such loss is first discovered by the insured and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM** and must occur after the "retroactive date" and before the end of the "policy period".

10. **Electronic Crime**
We will indemnify the "insured organization" for the loss of "money" or "securities", in excess of the applicable "retention", contained in a "transfer account" at a "financial institution" resulting directly from "funds transfer fraud" committed solely by a third party; provided that such loss must be discovered by the insured during the "policy period" and reported in writing to us during the "policy period" or as otherwise provided in **SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM** and must occur after the "retroactive date" and before the end of the "policy period".

SECTION II – DEFENSE AND SETTLEMENT OF CLAIMS

1. We shall have the right and duty to defend, subject to all provisions, terms and conditions of this Policy:
   A. any "claim" against the insured seeking "damages" which are payable under the terms of this Policy, even if any of the allegations of the "claim" are groundless, false or fraudulent; or
   B. under **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties**, any "claim" in the form of a "regulatory proceeding".

   Selection of defense counsel shall be mutually agreed upon between the "named insured" and us; provided, however, that in the absence of such agreement, our decision as to the selection of defense counsel shall be final.

2. With respect to any "claim" against the insured seeking "damages" or "penalties" which are payable under this Policy, we will pay "claims expenses" incurred with our prior written consent. The limit of liability available to pay "damages" and "penalties" shall be reduced and may be completely exhausted by payment of "claims expenses". "Damages", "penalties" and "claims expenses" shall be applied against each "claim" "retention" payable by the insured as set forth in the "Policy Declarations".

3. If the insured refuses to consent to any settlement or compromise recommended by us and acceptable to the claimant and elects to contest the "claim", our liability for any "damages", "penalties", and "claims expenses" shall not exceed:
   A. the amount for which the "claim" could have been settled, less the remaining "retention", plus the "claims expenses" incurred up to the time of such refusal; plus
   B. fifty percent (50%) of any "claims expenses" incurred after the date such settlement or compromise was recommended to the insured plus fifty percent (50%) of any damages above the amount for which the "claim" could have been settled. The remaining fifty percent (50%) of such "claims expenses" and "damages" must be borne by the insured at their own risk and uninsured;

   or the applicable limit of liability, whichever is less, and we shall have the right to withdraw from further defense thereof by tendering control of said defense to the insured. The portion of any proposed settlement or compromise that requires the insured to cease, limit or refrain from actual or alleged infringing or otherwise injurious activity or is attributable to future royalties or other amounts that are not "damages" (or "penalties" for "claims" covered under **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties**) shall not be considered in determining the amount for which a "claim" could have been settled.

4. We agree that the insured may settle any "claim" where the "damages", "penalties" and "claims expenses" do not exceed the "retention", provided that the entire "claim" is resolved and the insured obtains a full release on behalf of all insureds from all claimants.

SECTION III – INSURED AND THE INSURED ORGANIZATION

Whether expressed in the singular or plural, "insured" shall mean:

1. The "named insured" and any "subsidiaries" of the "named insured" (together the "insured organization");

2. A director, manager of a limited liability company ("manager") or officer of the "insured organization", but only with respect to the performance of his or her duties as such on behalf of the "insured organization";

3. An "employee" of the "insured organization" (including a part-time or temporary "employee"), but only for work done while acting within the scope of his or her employment and related to the conduct of the "insured organization's" business;

4. An independent contractor (including a part-time or temporary attorney, paralegal or employee), but only for work done while acting within the scope of his or her employment and related to the conduct of the "insured organization's" business;

5. A principal if the "named insured" is a sole proprietorship, or a partner if the "named insured" is a partnership, but only with respect to the performance of their duties as such on behalf of the "insured organization";

6. Any person previously qualified as an insured under paragraphs 2., 3., 4. or 5. of this section prior to the termination of the required relationship with the "insured organization", but only with respect to the performance of his or her duties as such on behalf of the "insured organization";

7. The estate, heirs, executors, administrators, assigns and legal representatives of any insured in the event of such insured's death, incapacity, insolvency or bankruptcy, but only to the extent that such insured would otherwise be provided coverage under this Policy; and

8. The lawful spouse, including any natural person qualifying as a domestic partner under the provisions of any applicable federal, state, or local law in the United States, of any insured, but solely by reason of any act, error or omission of an insured other than such spouse or domestic partner.

SECTION IV – EXCLUSIONS

This coverage does not apply to any "claim" or "loss":

1. For, arising out of or resulting from:
   A. physical injury, sickness, disease or death of any person, including any mental anguish or emotional distress resulting from such physical injury, sickness, disease or death; or
   B. physical injury to or destruction of any tangible property, including the loss of use thereof; provided that electronic data shall not be considered tangible property for purposes of this exclusion.

2. For, arising out of or resulting from any employer-employee relations, policies, practices, acts or omissions, or any actual or alleged refusal to employ any person, or misconduct with respect to employees, whether such "claim" is brought by an employee, former employee, applicant for employment, or relative or domestic partner of such person; provided, that this exclusion shall not apply to an otherwise covered "claim" under paragraph A. or B. under **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** by a current or former "employee" of the "insured organization", or to the providing of privacy breach response services involving current or former "employees" of the "insured organization".

3. For, arising out of or resulting from any actual or alleged act, error or omission or breach of duty by any director, officer or "manager" in the discharge of their duty if the "claim" is brought by or on behalf of the "named insured", a "subsidiary", or any principals, directors, officers, "managers", stockholders, members or "employees" of the "named insured" or a "subsidiary" in his or her capacity as such.

4. For, arising out of or resulting from any contractual liability or obligation or arising out of or resulting from breach of contract or agreement, either oral or written; however, this exclusion will not apply:

A. with respect only to the coverage provided pursuant to paragraph A. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**, to any obligation of the "insured organization" to maintain the confidentiality or security of "personally identifiable information" or of "third party information";
B. with respect only to paragraph D. of **SECTION I – INSURING AGREEMENTS, 4. Website Media Content Liability**, for misappropriation of ideas under implied contract;
C. to "computer expert services" or "legal services" covered under **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services**;
D. to "PCI fines, expenses & costs" covered under **SECTION I – INSURING AGREEMENTS, 5. PCI Fines, Expenses and Costs**, or
E. to the extent the insured would have been liable in the absence of such contract or agreement.

5. For, arising out of or resulting from any actual or alleged antitrust violation, restraint of trade, unfair competition, or false, deceptive or misleading advertising or violation of the Sherman Antitrust Act, the Clayton Act, or the Robinson-Patman Act, as amended.

6. For, arising out of or resulting from any actual or alleged false, deceptive or unfair trade practices; however, this exclusion does not apply to:
   A. any "claim" covered under paragraphs A., B. or C. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** or **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties**; or
   B. the provision of privacy breach response services covered under **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services**;

   that results from a theft, loss or "unauthorized disclosure" of "personally identifiable information" provided that no member of the "control group" participated or colluded in such theft, loss or "unauthorized disclosure".

7. For, arising out of or resulting from:
   A. the actual or alleged unlawful collection, acquisition or retention of "personally identifiable information" (except as otherwise covered under paragraph e. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**) or other personal information by, on behalf of, or with the consent or cooperation of the "insured organization"; or the failure to comply with a legal requirement to provide individuals with the ability to assent to or withhold assent (e.g. opt-in or opt-out) from the collection, disclosure or use of "personally identifiable information"; provided that this exclusion shall not apply to the actual or alleged unlawful collection, acquisition or retention of "personally identifiable information" by a person or entity that is not a "related party" and without the knowledge of the "insured organization"; or
   B. the distribution of unsolicited email, text messages, direct mail, or facsimiles, wiretapping, audio or video recording, or telemarketing, if such distribution, wiretapping or recording is done by or on behalf of the "insured organization".

8. For, arising out of or resulting from
   A. that which was the subject of written notice given to us or to any other insurer prior to the inception date of this coverage; or
   B. which was the subject of any prior and/or pending written demand made against any insured or a civil administrative or arbitration proceeding commenced against any insured, prior to the inception date of this coverage, or that involved the same or substantially the same fact, circumstance or situation underlying or alleged in such prior demand or proceeding.

9. For, arising out of or resulting from any related or continuing acts, errors, omissions, incidents or events where the first such act, error, omission, incident or event was committed or occurred prior to the "retroactive date".

10. For, arising out of resulting from any of the following:
    A. any actual or alleged violation of the Organized Crime Control Act of 1970 (commonly known as Racketeer Influenced and Corrupt Organizations Act or RICO), as amended;
    B. any actual or alleged violation of any securities law, regulation or legislation, including but not limited to the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Act of 1940, the Sarbanes-Oxley Act of 2002 or any "Blue Sky" laws;

C. any actual or alleged acts, errors or omissions related to any of the "insured organization's" pension, healthcare, welfare, profit sharing, mutual or investment plans, funds of trusts, including any violation of any provision of the Employee Retirement Income Security Act of 1974 (ERISA);

D. any actual or alleged violation of a regulation promulgated under any of the laws described in paragraphs A., B. or C. above; or

E. any actual or alleged violation of a federal, state, local or foreign laws or legislation similar to the laws described in paragraphs A., B. or C. above;

provided, however, this exclusion does not apply to any otherwise covered "claim" under paragraph A., B. or C. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** or to providing privacy breach response services covered under **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services**, that results from a theft, loss or "unauthorized disclosure" of "personally identifiable information", provided that no member of the "control group" participated or colluded in such theft, loss or "unauthorized disclosure".

11. Any actual or alleged discrimination of any kind including but not limited to age, color, race, sex, creed, national origin, marital status, sexual preference, disability or pregnancy.

12. Arising out of or resulting from any criminal, dishonest, fraudulent, or malicious act, error or omission, any intentional "security breach", intentional violation of a "privacy policy", or intentional or knowing violation of the law, if committed by such insured, or by others if the insured colluded or participated in any such conduct or activity; provided this exclusion shall not apply to:

A. "claims expenses" incurred in defending any "claim" alleging the foregoing until such time as there is a final non-appealable adjudication, judgment, binding arbitration decision or conviction against the insured, or written admission by the insured, establishing such conduct, or a plea of nolo contendere or no contest regarding such conduct, at which time the "named insured" shall reimburse us for all "claims expenses" incurred defending the "claim" and we shall have no further liability for "claims expenses; or

B. a "claim" or "loss" against a natural person insured if such insured did not personally commit, participate in or know about any act, error, omission, incident or event giving rise to such "claim" or "loss".

For purposes of this exclusion, only acts, errors, omissions or knowledge of a member of the "control group" will be imputed to the "insured organization".

13. For, arising out of or resulting from any actual or alleged:

A. infringement of patent or patent rights or misuse or abuse of patent or patent rights;

B. infringement of copyright arising from or related to software code or software products other than infringement resulting from a theft or "unauthorized access or use" of software code by a person who is not a "related party";

C. use or misappropriation of any ideas, trade secrets or third party corporate information by, or on behalf of, the "insured organization", or by any other person or entity if such use or misappropriation is done with the knowledge, consent or acquiescence of a member of the "control group";

D. disclosure, misuse or misappropriation of any ideas, trade secrets or confidential information that came into the possession of any person or entity prior to the date the person or entity became an employee, officer, director, "manager", principal, partner or "subsidiary" of the insured; or

E. under paragraph b. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**, theft of or "unauthorized disclosure" of a "data asset".

14. In connection with or resulting from a "claim" brought by or on behalf of the any state, federal, local or foreign governmental entity, in such entity's regulatory or official capacity; provided, this exclusion shall not apply to an otherwise covered "claim" under **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties** or to the provision of privacy breach response services under **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services** to the extent such services are legally required to comply with a "breach notice law".

15. For, arising out of or resulting from a "claim" by or on behalf of one or more insureds under this Policy against any other insured or insureds under this Policy, provided this exclusion shall not apply to an otherwise covered "claim" under paragraphs A., B. or C. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** made by a current or former "employee" of the "insured organization".

16. For, arising out of or resulting from:

A. any "claim" made by any business enterprise in which any insured has greater than a fifteen percent (15%) ownership interest or made by any parent company or other entity which owns more than fifteen percent (15%) of the "named insured"; or
B. the insured's activities as a trustee, partner, member, "manager", officer, director or employee of any employee trust, charitable organization, corporation, company or business other than that of the "insured organization".

17. For, arising out of or resulting from any of the following:
A. trading losses, trading liabilities or change in value of accounts;
B. any loss, transfer or theft of "monies", "securities" or tangible property of others in the care, custody or control of the "insured organization";
C. the monetary value of any transactions or electronic fund transfers by or on behalf of the insured which is lost, diminished, or damaged during transfer from, into or between accounts; or
D. the value of coupons, price discounts, prizes, awards, or any other valuable consideration given in excess of the total contracted or expected amount.

18. For, arising out of or resulting from:
A. the actual or alleged obligation to make licensing fees or royalty payments;
B. any costs or expenses incurred or to be incurred by the insured or others for the reprinting, reposting, recall, removal or disposal of any "media material" or any other information, content or media, including any media or products containing such "media material", information, content or media;
C. any "claim" brought by or on behalf of any intellectual property licensing bodies or organizations;
D. the actual or alleged inaccurate, inadequate or incomplete description of the price of goods, products or services, cost guarantees, cost representations, or contract price estimates, the authenticity of any goods, products or services, or the failure of any goods or services to conform with any represented quality or performance;
E. any actual or alleged gambling, contest, lottery, promotional game or other game of chance; or
F. any "claim" made by or on behalf of any independent contractor, joint venture or venture partner arising out of or resulting from disputes over ownership of rights in "media material" or services provided by such independent contractor, joint venture or venture partner.

19. For, arising out of or resulting from, directly or indirectly occasioned by, happening through or in consequence of: war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority; provided that this exclusion will not apply to cyber terrorism. For purposes of this exclusion, cyber terrorism means the premeditated use of disruptive activities, or threat to use disruptive activities, against a computer system of network with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

20. Either in whole or in part, directly or indirectly arising out of or resulting from or in consequence of, or in any way involving:
A. asbestos, or any materials containing asbestos in whatever form or quantity;
B. the actual, potential, alleged or threatened formation, growth, presence, release or dispersal of any fungi, molds, spores or mycotoxins of any kind; any action taken by any party in response to the actual, potential, alleged or threatened formation, growth, presence, release or dispersal of fungi, molds, spores or mycotoxins of any kind, such action to include investigating, testing for, detection of, monitoring of, treating, remediating or removing such fungi, molds, spores or mycotoxins; and any governmental or regulatory order, requirement, directive, mandate or decree that any party take action in response to the actual, potential, alleged or threatened formation, growth, presence, release or dispersal of fungi, molds, spores or mycotoxins of any kind, such action to include investigating, testing for, detection of, monitoring of, treating, remediating or removing such fungi, molds, spores or mycotoxins; we will have no duty or obligation to defend any insured with respect to any "claim" or governmental or regulatory order, requirement, directive, mandate or decree which either in whole or in part, directly or indirectly, arises out of or results from or in consequence of, or in any way involves the actual, potential, alleged or threatened formation, growth, presence, release or dispersal of any fungi, molds, spores or mycotoxins of any kind;
C. the existence, emission or discharge of any electromagnetic field, electromagnetic radiation or electromagnetism that actually or allegedly affects the health, safety or condition of any person or the environment, or that affects the value, marketability, condition or use of any property; or

D. the actual, alleged or threatened discharge, dispersal, release or escape of pollutants; or any governmental, judicial or regulatory directive or request that the insured or anyone acting under the direction or control of the insured test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants. Pollutants means any solid, liquid, gaseous or thermal irritant or contaminant including gas, acids, alkalis, chemicals, heat, smoke, vapor, soot, fumes or waste. Waste includes but is not limited to materials to be recycled, reconditioned or reclaimed.

21. With respect to **SECTION I – INSURING AGREEMENTS, 7. First Party Data Protection** and **8. First Party Network Business Interruption**, for, arising out of or resulting from:
    A. any failure or malfunction of electrical or telecommunication infrastructure or services, provided that this exclusion shall not apply to any otherwise covered "claim" or "loss" arising out of failure of "computer security" to prevent a "security breach" that was solely caused by a failure or malfunction of telecommunications infrastructure or services under the insured's direct operational control;
    B. fire, flood, earthquake, volcanic eruption, explosion, lightning, wind, hail, tidal wave, landslide, act of God or other physical event; or
    C. any satellite failures.

22. With respect to **SECTION I – INSURING AGREEMENTS, 6. Cyber Extortion**, for, arising out of or resulting from:
    A. any threat to physically harm or kidnap any person; or
    B. any threat to harm, take, or transfer property other than any "data asset", even if such threat is made in conjunction with a threat to a "data asset".

23. With respect to **SECTION I – INSURING AGREEMENTS, 6. Cyber Extortion**, for, arising out of or resulting from an "extortion threat" first made against the "insured organization" during the "policy period" by any of the "insured organization's" directors, officers, principals, trustees, governors, "managers", members, management committee members, members of the management board, partners, or any person in collusion with any of the foregoing.

24. Arising out of or resulting from any seizure, nationalization, confiscation or destruction of "computer systems" or "data assets" by order of any governmental or public authority.

25. For, arising out of or resulting from a "claim" covered by any other professional liability insurance available to any insured, including, but not necessarily limited to, any self-insured retention or deductible portion thereof, and including any other insurance policy that we have issued to the "named insured".

26. For, arising out of or resulting from any of the following:
    A. trading losses, trading liabilities or change in value of accounts;
    B. any loss, transfer or theft of "monies", "securities" or tangible property of others in the care, custody or control of the "insured organization";
    C. the monetary value of any transactions or electronic fund transfers by or on behalf of the insured which is lost, diminished, or damaged during transfer from, into or between accounts; or
    D. the value of coupons, price discounts, prizes, awards, or any other valuable consideration given in excess of the total contracted or expected amount; provided that subsections A., B. and C. of this exclusion shall not apply to "loss" covered under **SECTION I- INSURING AGREEMENTS, 9. Fraudulent Instruction or 10. Electronic Crime.**

27. With respect to **SECTION I – INSURING AGREEMENTS, 9. Fraudulent Instruction**, for, arising out of or resulting from, either directly or indirectly:
    A. the actual or alleged use of credit, debit, charge, access, convenience, customer identification or other cards;
    B. any transfer of money, goods, information or other item involving any person or entity that had authorized access to the insured's authentication mechanism;
    C. the processing of, or the failure to process, credit, check, debit, personal identification number debit, electronic benefit transfers or mobile payments for merchant accounts;
    D. any "fraudulent instruction" that was not verified with the requestor using an "out-of-band authentication";
    E. the failure of any party to perform, in whole or in part, under any contract or agreement;
    F. the failure, malfunction, inadequacy or illegitimacy of any product or service;
    G. accounting or arithmetical errors or omissions;
    H. indirect or consequential loss of any kind including income not realized as the result of a covered loss; or

I. fees, costs or expenses incurred in defending or prosecuting any legal proceeding or claim;
J. any transfer of "money" or "securities" to a third party or vendor where the received funds are being returned before having cleared the insured's bank account.

28. With respect to **SECTION I – INSURING AGREEMENTS, 10. Electronic Crime**, for, arising out of or resulting from, either directly or indirectly:
A. the type or kind covered by the "insured organization's" financial institution bond or commercial crime policy, regardless of any deductible amount or limit of liability;
B. any actual or alleged fraudulent, dishonest or criminal act or omission by any "employee", whether acting alone or in collusion with any other person or entity;
C. indirect or consequential loss of any kind;
D. punitive, exemplary or multiplied damages of any kind or any fines, penalties or loss of any tax benefit;
E. the giving or surrendering of any "money" or "securities" in any exchange or purchase, whether fraudulent or not;
F. fees, costs or expenses incurred or paid by the "insured organization" in defending or prosecuting any legal proceeding or claim;
G. proving or establishing the existence of loss under this Policy;
H. the theft, disappearance, destruction of, or unauthorized access to, confidential information including, but not limited to, trade secrets, customer lists, and intellectual property;
I. any "fraudulent instruction" if the sender, or anyone acting in collusion with the sender, ever had access to the "insured organization's" password, pin or other security code;
J. any forged, altered or fraudulent negotiable instruments, "securities", documents or instructions;
K. any actual or alleged use of credit, debit, charge, access, convenience or other cards or the information contained on such cards;
L. damages of any type for which the "insured organization" is legally liable, except for direct compensatory damages arising directly from "funds transfer fraud"; or
M. costs or expenses incurred by a customer or client of the "insured organization".

SECTION V – LIMITS OF LIABILITY AND COVERAGE

1. The policy aggregate limit of liability set forth in the "Policy Declarations" is our combined total limit of liability for all "damages", "penalties", "PCI fines, expenses and costs", "cyber extortion loss", "data protection loss", "business interruption loss", "claims expenses" and loss under **Section I – Insuring Agreements, 9. Fraudulent Instruction and 10. Electronic Crime** payable under this Policy.

2. The Information Security and Privacy Liability sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** of this Policy and is part of and not in addition to the policy aggregate limit of liability.

3. The Regulatory Defense and Penalties sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties** of this Policy and is part of and not in addition to the policy aggregate limit of liability.

4. The Website Media Content Liability sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 4. Website Media Content Liability** of this Policy and is part of and not in addition to the policy aggregate limit of liability.

5. The PCI Fines, Expenses and Costs sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 5. PCI Fines, Expenses and Costs** of this Policy and is part of and not in addition to the policy aggregate limit of liability.

6. The Cyber Extortion sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 6. Cyber Extortion** of this Policy and is part of and not in addition to the policy aggregate limit of liability. Multiple related or continuing "extortion threats" shall be considered a single "extortion threat" for purposes of this Policy and shall be deemed to have occurred at the time of the first such "extortion threat".

Prior to the payment of any "extortion payment", the "insured organization" shall make every reasonable effort to determine that the "extortion threat" is not a hoax, or otherwise not credible. The "insured organization" shall take all steps reasonable and practical to avoid or limit the payment of an "extortion payment".

7. The First Party Data Protection sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 7. First Party Data Protection** of this Policy and is part of and not in addition to the policy aggregate limit of liability. A "data protection loss" will be deemed to occur at the time such alteration, corruption, destruction, deletion of damage to or inability to access a "data asset" is first discovered by the insured. All "data protection loss" that arises out of the same or a continuing "security breach", from related or repeated "security breaches", or from multiple "security breaches" resulting from a failure of "computer security" shall be deemed to be a single "data protection loss".

8. The First Party Network Business Interruption sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 8. First Party Network Business Interruption** of this Policy and is part of and not in addition to the policy aggregate limit of liability. All "business interruption loss" resulting from multiple covered interruptions of "computer systems" that arise out of the same or a continuing "security breach", from related or repeated "security breaches", or from multiple "security breaches" resulting from a failure of "computer security" shall be deemed to be a single "business interruption loss"; provided, however, that a separate "waiting period" shall apply to each "period of restoration".

9. The Fraudulent Instruction sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 9. Fraudulent Instruction** of this Policy and is part of and not in addition to the policy aggregate limit of liability. All losses arising out of or resulting from the same "fraudulent instruction", multiple or series of "fraudulent instructions" purporting to be from the same "vendor", "client" or "authorized employee" or related "vendors", "clients" or "authorized employees", or multiple or a series of "fraudulent instructions" from the same third party or related third parties shall be deemed to be each a single loss under this Policy subject to the "retention".

10. The Electronic Crime sublimit of liability stated in the "Policy Declarations" is the aggregate sublimit of liability payable under **SECTION I – INSURING AGREEMENTS, 10. Electronic Crime** of this Policy and is part of and not in addition to the policy aggregate limit of liability.

11. Neither the inclusion of more than one insured under this Policy, nor the making of "claims" by more than one person or entity shall increase the sublimit of liability or policy aggregate limit of liability.

12. The limit of liability for the optional "extended reporting period" shall be part of and not in addition to the policy aggregate limit of liability.

13. We shall not be obligated to pay any "damages", "penalties", "PCI Fines, Expenses and Costs" or "claims expenses", or to undertake or continue defense of any suit or proceeding after the policy aggregate limit of liability has been exhausted by payment of "damages", "penalties", "PCI Fines, Expenses and Costs", "cyber extortion loss", "data protection loss", "business interruption loss", "claims expenses" or loss under **Section I – Insuring Agreements, 9. Fraudulent Instruction and 10. Electronic Crime**, or after deposit of the policy aggregate limit of liability in a court of competent jurisdiction. Upon such payment, we shall have the right to withdraw from further defense of any "claim" under this Policy by tendering control of said defense to the insured.

14. The "notified individuals" limit stated in the "Policy Declarations" is the maximum total number of "notified individuals" to whom notification will be provided or attempted for all incidents or series of related incidents giving rise to an obligation to provide "notification services", "call center services" or "breach resolution and mitigation services".

15. The aggregate limit of coverage stated for "computer expert services", "legal services" and "public relations and crisis management expenses" in the "Policy Declarations" is the aggregate limit of coverage for all "computer expert services", "legal services" and "public relations and crisis management expenses" combined. This is a separate limit, apart from and in addition to the policy aggregate limit of liability.

16. If the total number of notifications made pursuant to paragraph D. of **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services** aggregates to more than the "notified individuals" limit of coverage stated in the "Policy Declarations", the "insured organization" will be responsible for paying for privacy breach response services with respect to any excess notification, and such costs will not be covered under this Policy. If an incident involves notifications made pursuant to paragraph C. of **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services** both within the "notified individuals" limit of coverage stated in the "Policy Declarations" and in excess of such limit, all excess notifications will be provided by the same service provider that provides "notification services" covered under this Policy, and the costs will be allocated between us and the "insured organization" pro rata based on the number of covered and non-covered notifications.

17. To the extent privacy breach response services costs are covered pursuant to a "claim" as described in paragraph 5.D. of **SECTION XXIV – DEFINITIONS**, such costs shall be covered solely under **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability.**

SECTION VI – RETENTION

1. The "retention" amount set forth in the "Policy Declarations" applies separately to each incident, event or related incidents or events giving rise to a "claim". The "retention" shall be satisfied by monetary payments by the "named insured" of "damages", "claims expenses", "penalties" or "PCI Fines, Expenses & Costs".

2. For "notification services", "call center services" and "breach resolution and mitigation services" for each incident, the "notified individuals" "retention" amount set forth in the "Policy Declarations" applies separately to each incident, event or related incidents or events giving rise to an obligation to provide such services.
3. For all "computer expert services", "legal services" and "public relations and crisis management services", the "retention" amount set forth in the "Policy Declarations" apply separately to each incident, event or related incidents or events, giving rise to an obligation to provide such services; and the applicable "retention" stated in the "Policy Declarations" shall be satisfied by monetary payments by the "named insured" for such services.

4. With respect to **SECTION I – INSURING AGREEMENTS, 6. Cyber Extortion**, the "retention" set forth in the "Policy Declarations" applies separately to each "extortion threat". The "retention" shall be satisfied by monetary payments by the "named insured" of covered "cyber extortion loss".

5. With respect to **SECTION I – INSURING AGREEMENTS, 7. First Party Data Protection**, the "retention" set forth in the "Policy Declarations" applies separately to each "security breach". The "retention" shall be satisfied by monetary payments by the "named insured" of covered "data protection loss".

6. With respect to **SECTION I – INSURING AGREEMENTS, 8. First Party Network Business Interruption,** the "retention" set forth in the "Policy Declarations" applies separately to each "security breach". The "retention" shall be satisfied by covered "business interruption loss" retained by the "insured organization". The "retention" applicable to **SECTION I – INSURING AGREEMENTS, 8. First Party Network Business Interruption** shall be reduced on a dollar-for-dollar basis by the amount of "income loss" that was sustained by the "insured organization" during the "waiting period".

7. With respect to **SECTION I – INSURING AGREEMENTS, 9. Fraudulent Instruction** and **10. Electronic Crime**, the "retention" amount set forth in the "Policy Declarations" applies separately to each incident, event, or related incidents or events, giving rise to an obligation to pay loss under these insuring agreements.
8. In the event that a "damages", "claims expenses", "penalties" or "PCI Fines, Expenses and Costs" arising out of a "claim" are subject to more than one "retention", the applicable "retention" amount shall apply to such "damages", "claims expenses", "penalties" or "PCI Fines, Expenses and Costs", provided, that the sum of such "retention" amounts shall not exceed the largest applicable "retention" amount.

9. In the event that "cyber extortion loss", "data protection loss" or "business interruption loss" arising out of a single incident are subject to more than one "retention", the applicable "retention" amounts shall apply to such "cyber extortion loss", "data protection loss" or "business interruption loss", provided that the sum of such "retention" amounts shall not exceed the largest applicable "retention" amount.

10. Satisfaction of the applicable "retention" is required prior to the payment by us of any amounts or providing of any services hereunder, and we shall be liable only for the amounts in excess of such "retention" subject to our total liability not exceeding the policy aggregate limit of liability or limit for privacy breach response services set forth in the "Policy Declarations". The "named insured" shall make direct payments within the "retention" to appropriate other parties designated by us.

SECTION VII– OPTIONAL EXTENDED REPORTING PERIOD

1. In the event that coverage under this Policy is cancelled, non-renewed or terminates for any reason except the non-payment of premium or "retention" due under this Policy, the "named insured" shall have the right, upon payment in full of the of the percentage of the premium set forth in the "Policy Declarations", to have issued an endorsement providing an optional "extended reporting period" for the period of time set forth in the "Policy Declarations" for "claims" first made against any insured and reported to us during the optional "extended reporting period" and arising out of any act, error or omission committed on or after the "retroactive date" and before the end of the "policy period", subject to the conditions set forth herein.

2. The optional "extended reporting period" does not apply to **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services, 6. Cyber Extortion, 7. First Party Data Protection, 8. First Party Network Business Interruption, 9. Fraudulent Instruction** or **10. Electronic Crime.**

3. In order for the "named insured" to invoke the optional "extended reporting period", written notice must be sent and the payment of the additional premium for the optional "extended reporting period" must be paid to us within thirty (30) days of the of the cancellation, non-renewal or termination of this this Policy. If notice of election of the optional "extended reporting period" is not given to us within such thirty (30) day period, there shall be no right to purchase the optional "extended reporting period".

4. The limit of liability for the optional "extended reporting period" shall be part of, and not in addition to, the applicable policy aggregate limit of liability for the "policy period". The purchase of the optional "extended reporting period" shall not in any way increase the policy aggregate limit of liability or any sublimit of liability.

5. The optional "extended reporting period" does not extend the "policy period" or change the scope of coverage provided under this Policy. The optional "extended reporting period" simply extends the reporting period during which a "claim" may be first reported to us under this Policy. Any "claim" reported to us during the optional "extended reporting period" shall be treated as if reported during the "policy period".

6. At the commencement of the optional "extended reporting period" the entire premium shall be deemed earned, and in the event the "named insured" cancels or terminates the optional "extended reporting period" for any reason prior to its natural expiration, we will not be liable to return any premium paid for the optional "extended reporting period".

SECTION VIII – NOTICE AND DUTIES IN THE EVENT OF A CLAIM, LOSS OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM

1. With respect to **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability, 3. Regulatory Defense and Penalties, 4. Website Media Content Liability** and **5. PCI Fines, Expenses and Costs**:
   - **A.** If any "claim" is made against the insured, the insured shall forward as soon as practicable to us written notice of such "claim" by facsimile, email or express or certified mail, together with every demand, notice, summons or other process received by the insured or the insured's representative. In no event shall we be given notice of a "claim" later than the end of the "policy period", the end of the optional "extended reporting period", if applicable, or sixty (60) days after the expiration date of the "policy period".
   - **B.** If, during the "policy period", the insured becomes aware of any circumstance that could reasonably be the basis for a "claim", it may give written notice to us in the form of a facsimile, email or express or certified mail as soon as practicable during the "policy period". Such notice must include:
     - **i.** the specific details of the act, error, omission, or "security breach" that could reasonably be the basis for a "claim";
     - **ii.** the injury or damage which may result or has resulted from the circumstance; and
     - **iii.** the facts by which the insured first became aware of the act, error, omission or "security breach".

Any subsequent "claim" made against the insured arising out of such circumstance which is the subject of the written notice will be deemed to have been made at the time written notice complying with the above requirements was first given to us.

C. A "claim" or legal obligation under paragraph a. of this section shall be considered to be reported to us when written notice is first received by us in the form of a facsimile, email or express or certified mail of the "claim" or legal obligation, or of an act, error, or omission, which could reasonably be expected to give rise to a "claim" if provided in compliance with this paragraph.

D. In the event coverage is renewed by us and privacy breach response services are provided because of such incident or suspected incident that was discovered by the insured prior to the expiration of this coverage, and first reported during the sixty (60) day post "policy period" reporting period, then any subsequent "claim" arising out of such incident or suspected incident is deemed to have been made during the "policy period".

2. With respect to **SECTION I – INSURING AGREEMENT, 2. Privacy Breach Response Services** and **6. Cyber Extortion**:

A. If any incident, or reasonably suspected incident, described in paragraphs a. or b. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** occurs, or in the event of a cyber extortion threat, the insured must report such incident, or reasonably suspected incident, to us in writing by facsimile, email or express or certified mail as soon as practicable during the "policy period" after discovery by the insured. In no event shall we be given notice of such incident later than the end of the "policy period" or sixty (60) days after the expiration date of the "policy period".

3. With respect to **SECTION I – INSURING AGREEMENT, 7. First Party Data Protection** and **8. First Party Network Business Interruption**:

A. Notice of "Data Protection Loss" or "Business Interruption Loss"

i. With respect to **SECTION I – INSURING AGREEMENT, 7. First Party Data Protection**, the "named insured" must forward written notice by facsimile, email or express or certified mail immediately upon discovery of alteration, corruption, destruction, deletion or damage to or inability to access a "data asset" to which this Policy applies. In no event shall we be given notice of "data protection loss" later than the end of the "policy period" or sixty (60) days after the expiration date of the "policy period".

ii. With respect to **SECTION I – INSURING AGREEMENT, 8. First Party Network Business Interruption**, the "named insured" must forward written notice by facsimile, email or express or certified mail immediately upon discovery of the interruption or suspension of "computer systems" to which this Policy applies. In no event shall we be given notice of "business interruption loss" later than the end of the "policy period" or sixty (60) days after the expiration date of the "policy period".

B. Proof of Loss & Appraisal

i. Before coverage will apply, the "named insured" must prepare and submit to us a written and detailed proof of loss sworn by an officer of the "named insured" within ninety (90) days after the insured discovers a "data protection loss" or the "insured organization" sustains a "business interruption loss", as applicable, but in no event later than six (6) months following the end of the "policy period" (unless such period has been extended by our written consent). Such proof of loss shall include a narrative with full particulars of such "data protection loss" or "business interruption loss", including, the time, place and cause of the "data protection loss" or "business interruption loss", a detailed calculation of any "data protection loss" or "business interruption loss", the "insured organization's" interest and the interest of all others in the property, the sound value thereof and the amount of "data protection loss" or "business interruption loss" or damage thereto and all other insurance thereon.

ii. The "named insured" must, upon our request, submit to an examination under oath and provide copies of the underlying documents, data and materials that reasonably relate to or are part of the basis of the claim for such "data protection loss" or "business interruption loss". The costs and expenses of preparing and submitting a proof of loss, and establishing or proving "data protection loss", "business interruption loss" or any other "loss" under this Policy shall be the insured's obligation.

iii. If we do not agree with the "named insured" on the amount of a "data protection loss" or a "business interruption loss", each party shall select and pay a qualified and disinterested appraiser or other qualified expert (the "Appraiser(s)") to state the amount of the loss or reasonable expenses, and the Appraisers shall choose an umpire. If the Appraisers cannot agree on an umpire, the "named insured" or we may request a judge of a court having jurisdiction to make the selection. Each Appraiser shall submit their loss estimate to the umpire, and agreement by the umpire and at least one of the Appraisers as to the amount of a "data protection

loss" or "business interruption loss" shall be binding on all insureds and us. The "named insured" and we will equally share the costs of the umpire and any other costs other than the cost of the Appraisers. This provision shall govern only appraisal under this section and shall not control the determination of whether such "data protection loss" or "business interruption loss" is otherwise covered by this Policy. We retain and do not waive our right to deny coverage or to enforce any obligation under this Policy.

4. With respect to **SECTION I – INSURING AGREEMENTS, 9. Fraudulent Instruction** and **10. Electronic Crime**:
   A. If the "named insured" sustains any loss of "monies" or "securities" as described in **SECTION I – INSURING AGREEMENT, 9. Fraudulent Instruction** or **10. Electronic Crime**, the insured must report such loss to us in writing by facsimile, email or express or certified mail as soon as practicable during the "policy period" after discovery by the insured. In no event shall we be given notice of such loss later than the end of the "policy period" or sixty (60) days after the expiration date of the "policy period".
   B. Before coverage under **SECTION I – INSURING AGREEMENTS, 9. Fraudulent Instruction** or **10. Electronic Crime** will apply, the "named insured" must prepare and submit to us a proof of loss, duly sworn to, within sixty (60) days after the insured discovered such loss. Such proof of loss shall include any available documentation of fraudulent written, electronic or telephone instructions, documentation of verification via a method other than the original means of the request, the amount of loss incurred, and all other insurance available to the insured in connection with such loss.

SECTION IX – POLICY TERRITORY

This Policy applies to any act, error or omission occurring anywhere in the world, provided that a Claim otherwise covered by this Policy is made within the United States of America, its territories or possessions, or Canada.

SECTION X – ASSISTANCE AND COOPERATION

1. We shall have the right to make any investigation we deem necessary, and the insured shall cooperate fully with us in all investigations for and coverage under this Policy. The insured shall execute or cause to be executed all papers and render all assistance as we request. The insured agrees not to take any action which in any way increases our exposure under this Policy.

2. Upon our request, the insured shall assist in making settlements, in the conduct of suits and in enforcing any right of contribution or indemnity against any person or organization who may be liable to the insured because of acts, errors or omissions, incidents or events with respect to which insurance is afforded under this Policy; and the insured shall attend hearings and trials and assist in securing and giving evidence and obtaining the attendance of witnesses.

3. The insured shall not admit liability, make any payment, assume any obligations, incur any expense, enter into any settlement, stipulate to any judgment or award or dispose of any "claim" without our written consent, except as specifically provided in **Section II – DEFENSE AND SETTLEMENT OF CLAIMS**, paragraph 4 of this Policy. Compliance with a Breach Notice Law will not be considered as an admission of liability for purposes of this Clause XI.C.

4. Expenses incurred by the insured in assisting and cooperating with us do not constitute "claims expenses" under the Policy.

SECTION XI – ACTION AGAINST THE UNDERWRITERS

1. No action shall lie against us or our representatives unless and until, as a condition precedent thereto, the insured shall have fully complied with all provisions, terms and conditions of this Policy and the amount of the insured's obligation to pay shall have been finally determined either by judgment or award against the insured after trial, regulatory proceeding, arbitration or by written agreement of the insured, the claimant, and us.

2. No person or organization shall have the right under this Policy to join us as a party to an action or other proceeding against the insured to determine the insured's liability, nor shall we be impleaded by the insured or the insured's legal representative.

SECTION XII – ACQUISITIONS AND MERGERS

1. Newly Acquired Subsidiaries.
   A. During the Policy Period, if the "named insured" or any "subsidiary" acquires another entity whose annual revenues are more than ten percent (10%) of the "named insured's" total annual revenues for the four quarterly periods directly preceding inception of the "policy period", such acquired entity shall not be a "subsidiary", and no insured shall have coverage under this Policy for any "claim" or "loss" that arises out of any act, error omission, incident or event whether committed before or after such acquisition:
      i. by or on behalf of the acquired entity or any person employed by the acquired entity;
      ii. involving or relating to the assets, liabilities, activities or policies or procedures of the acquired entity or to data, information, computers, or networks, security systems, of or under the care, custody or control of the acquired entity, a business associate of the acquired entity, or a third party on behalf of the acquired entity; or
      iii. by any person or entity holding, processing, managing or transferring information or operating "computer systems" on behalf of the acquired entity;

   unless the "named insured" gives us written notice prior to the acquisition, obtains our prior written consent to extend coverage to such additional entities, assets, exposures, or "computer systems", and agrees to pay any additional premium we require.

   If during the "policy period" the "named insured" or any "subsidiary" acquires a privately held entity whose annual revenues are more than ten percent (10%) of the "named insured's" total annual revenues for the four quarterly periods directly preceding inception of the "policy period", then, subject to the "policy period" and all other terms and conditions of this Policy, coverage under this Policy shall be afforded for a period of sixty (60) days, but only for any "claim" that arises out of any act, error or omission first committed or incident or event first occurring after the entity becomes so owned. Coverage beyond such sixty (60) day period shall only be available if the "named insured" gives us written notice prior to the acquisition, obtains our prior written consent to extend coverage to such additional entities, assets, exposures, or "computer systems", and agrees to pay any additional premium we require.

2. Mergers or Consolidations.

If during the "policy period" the "named insured" consolidates or merges with or is acquired by another entity, or sells substantially all of its assets to any other entity, then this Policy shall remain in full force and effect, but only with respect to a "security breach", or other act or incidents that occur prior to the date of the consolidation, merger or acquisition. There shall be no coverage provided by this Policy for any other "claim" or "loss" unless the "named insured" provides written notice to us prior to such consolidation, merger or acquisition, the "named insured" has agreed to pay any additional premium and terms of coverage we require, and we have issued an endorsement extending coverage under this Policy.

SECTION XIII – ASSIGNMENT

No rights or interests hereunder of any insured may be assigned. If the insured shall die or be adjudged incompetent, such insurance shall cover the insured's legal representative as the insured as would be permitted under this Policy.

SECTION XIV – CANCELLATION AND NON-RENEWAL

1. The "named insured" may cancel this Policy at any time upon surrender of the Policy to us or by mailing or delivering to us a written notice stating when the cancellation shall be effective.

2. We may cancel this Policy by mailing or delivering to the "named insured" at the address shown in the "Policy Declarations" written notice stating when, not less than sixty (60) days thereafter, such cancellation shall be effective. However, in the event the "named insured" has failed to pay when due a premium or "retention" due under this Policy, or any other money owed to us, we may cancel this Policy by written notice of cancellation to the "named insured" stating the date upon which the cancellation will be effective, which date shall be no fewer than ten days following the date of the notice. Such notice shall be effective and conclusive as to all insureds hereunder. Proof of mailing shall be sufficient proof of notice and the effective date of cancellation stated in the notice shall become the end date of the "policy period". Delivery (where permitted by law) of such written notice either by the "named insured" or by us shall be equivalent of mailing.

3. If the "named insured" cancels this Policy, the earned premium shall be computed in accordance with the customary short rate tables and procedures.

4. If we cancel this Policy, earned premium shall be computed pro rata.

5. Premium adjustment may be made either at the time cancellation is effected or as soon as practicable after cancellation becomes effective, but payment or tender of unearned premium is not a condition of cancellation.

6. If we elect not to renew this Policy, we shall provide the "named insured with no less than sixty (60) days advance written notice thereof.

SECTION XV – SINGULAR FORM OF A WORD

Whenever the singular form of a word is used herein, the same shall include the plural when required by context.

SECTION XVI – HEADINGS

The titles of paragraphs, section, provisions, or endorsements of or to this Policy are intended solely for convenience and reference, and are not deemed in any way to limit or expand the provisions to which they relate and are not part of the Policy.

SECTION XVIII – NAMED INSURED AS AGENT

All insureds agree that the "named insured" shall be considered the agent of all insureds, and shall act on behalf of all insureds with respect to the giving of or receipt of all notices pertaining to this Policy, the acceptance of any endorsements to this Policy, and the "named insured" shall be responsible for the payment of all premiums and "retentions" as well as the receipt of any return Premiums.

SECTION XIX – BANKRUPTCY

Bankruptcy or insolvency of any insured or of an insured's estate will not relieve us of our obligations under this Policy.

SECTION XX – OTHER INSURANCE

The coverage under this Policy shall apply in excess of any other valid and collectible insurance available to any insured, including any self-insured retention or deductible portion thereof, unless such other insurance is written, only as specific excess insurance over the policy aggregate limit of liability or any other applicable limit of liability or coverage of this Policy.

SECTION XXI – SUBROGATION

If any payment is made under this Policy and there is available to us any of the insured's rights of recovery against any other party, then we shall maintain all such rights of recovery. The insured shall execute and deliver instruments and papers and do whatever else is necessary to secure such rights. The insured shall do nothing after an incident or event giving rise to a "claim" or "loss" to prejudice such rights. Any recoveries shall be applied first to subrogation expenses, second to "loss" paid by us and lastly to the "retention". Any additional amounts recovered shall be paid to the "named insured".

SECTION XXII – NOTICES

All notices to be delivered to the "named insured" under this Policy shall be mailed first class postage to the "named insured" at the address shown in Item 1 of the "Policy Declarations" unless we are notified in writing of a change in the mailing address of the "named insured". Except for notice of a "claim", which shall be delivered to us as indicated on Page 1 of this Policy, all other notices to be delivered to the Underwriters shall be mailed first class postage to the Insurer at the following address:

ALPS
111 North Higgins, Suite 600
P.O. Box 9169

SECTION XXIII – ENTIRE AGREEMENT

By acceptance of the Policy, all insureds agree that this Policy embodies all agreements between us and the 'insured" relating to this Policy. Notice to any agent or knowledge possessed by any agent or by any other person shall not effect a waiver or a change in any part of this Policy or prevent us from asserting any right under the terms of this Policy; nor shall the terms of this Policy be waived or changed, except by written endorsement issued to form a part of this Policy and signed by us.

SECTION XXIV – DEFINITIONS

1. "Authorized employee" means an employee who is authorized by the insured to transfer "money" or "securities" or to instruct other employees to transfer "money" or "securities".

2. "Breach notice law" means: any federal, state, local or foreign statute or regulation that requires notice to persons whose "personally identifiable information" was accessed or reasonably may have been accessed by an unauthorized person.

3. "Breach resolution and mitigation services" means a credit monitoring, identity monitoring or other solution offered to "notified individuals". The product offered to "notified individuals" will be selected from our panel by us in consultation with the "insured organization".

4. "Business interruption loss" means the actual "income loss", "forensic expenses" and "extra expense" incurred during the "period of restoration". "Business interruption loss" shall not include:
   A. "loss" arising out of any liability to any third party for whatever reason; legal costs or legal expenses of any type; "loss" incurred as a result of unfavorable business conditions, loss of market or any other consequential loss; or costs or expenses the "insured organization" incurs to identify or remove software program errors or vulnerabilities; or
   B. expenses incurred by the insured to update, upgrade, enhance or replace "computer systems" to a level beyond that which existed prior to the actual and necessary interruption of "computer systems"; or the costs and expenses incurred by the "insured organization" to restore, reproduce or regain access to any "data asset" that was altered, corrupted, destroyed, deleted, damaged or rendered inaccessible as a result of the failure of "computer security" to prevent a "security breach".

5. "Call center services" means the provision of a call center to answer calls during standard business hours for a period of ninety (90) days following notification (or longer if required by applicable law or regulation) of an incident for which notice is provided pursuant to paragraph d. of **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services**. "Call center services" will be provided by a service provider from our panel selected by us in consultation with the "insured organization".

6. "Claim" means:
   A. a written demand received by any insured for money or services, including service of a suit or institution of regulatory or arbitration proceedings;
   B. with respect to coverage provided under **SECTION I – INSURING AGREEMENTS, 3. Regulatory Defense and Penalties** only, institution of a "regulatory proceeding" against any insured;
   C. a written request or agreement to toll or waive a statute of limitations relating to a potential "claim" described in paragraph A. above; and
   D. with respect to coverage provided under paragraph a. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** only, a demand received by any insured to fulfill the "insured organization's" contractual obligation to provide notice of an incident, or reasonably suspected incident, described in paragraph A. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** pursuant to a "breach notice law".

   Multiple "claims" arising from the same or a series of related or repeated acts, errors, or omissions, or from any continuing acts, errors, omissions, or from multiple "security breaches" arising from a failure of "computer security" shall be considered a single "claim" for the purposes of this Policy, irrespective of the number of claimants or insureds involved in the "claim". All such "claims" shall be deemed to have been made at the time of the first such "claim".

7. "Claims expenses" means:
   A. reasonable and necessary fees charged by an attorney designated pursuant to paragraph 1. of **SECTION II – DEFENSE AND SETTLEMENT OF CLAIMS**;
   B. all other legal costs and expenses resulting from the investigation, adjustment, defense and appeal of a "claim", suit, or proceeding arising in connection therewith, or circumstance which might lead to a "claim" if incurred by us or the insured with our prior written consent;
   C. the premium cost for appeal bonds for covered judgments or bonds to release property used to secure a legal obligation, if required in any "claim" against an "insured' provided that we shall have no obligation to appeal or to obtain bonds.

   "Claims expenses" do not include any salary, overhead, or other charges by the insured for any time spent cooperating with the defense and investigation of any "claim", or circumstance that might lead to a "claim", under this Policy, or costs to comply with any regulatory orders, settlements or judgments.

8. "Client" means a customer of the insured to whom the insured provides goods or services under a written contract or for a fee.

9. "Computer expert services" means costs for:
   A. a computer security expert to determine the existence and cause of an actual or suspected electronic data breach which may require the "insured organization" to comply with a "breach notice law" and to determine the extent to which such information was accessed by an unauthorized person or persons; and if such breach is actively in progress on the "insured organization's" "computer systems", to assist in containing the existing intrusion on such systems from accessing "personally identifiable information"; and
   B. a Payment Card Industry (PCI) Forensic Investigator that is approved by the PCI Security Standards Council and is retained by the "insured organization" in order to comply with the terms of a "merchant services agreement" to investigate the existence and extent of an actual or suspected compromise of credit card data; and, in our discretion, where a computer security expert described in paragraph a. above has not been retained, for a computer security expert to provide advice and oversight in connection with the investigation conducted by the PCI Forensic Investigator; and
   C. a computer security expert to demonstrate the insured's ability to prevent a future electronic data breach as required by a "merchant services agreement".

   "Computer expert services" will be provided by a service provider from our panel selected by us in consultation with the "insured organization".

10. "Computer security" means software, computer or network hardware devices, as well as the "insured organization's" information security policies and procedures, the function or purpose of which is to prevent "unauthorized access or use", a "denial of service attack" against "computer systems", infection of "computer systems" by "malicious code" or transmission of "malicious code" from "computer systems". "Computer security" includes anti-virus and intrusion

detection software, firewalls and electronic systems that provide access control to "computer systems" through the use of passwords, biometric or similar identification of authorized users.

11. "Computer systems" means computers, any software residing on such computers, and associated input and output devices, data storage devices, networking equipment, and back up facilities:
    A. operated by and either owned by or leased to the "insured organization", or
    B. systems operated by a third party service provider and used for the purpose of providing hosted computer application services, including cloud services, to the "insured organization" or for processing, maintaining, hosting or storing the "insured organization's" electronic data, pursuant to written contract with the "insured organization" for such services.

12. "Control group" means any principal, partner, corporate officer, director, "manager", general counsel (or most senior legal counsel) or risk manager of the "insured organization" and any individual in a substantially similar position.

13. "Cyber extortion loss" means:
    A. any "extortion payment" that has been made under duress by or on behalf of the "insured organization", with our prior written consent, but solely to prevent or terminate an "extortion threat";
    B. reasonable and necessary expenses incurred by the "insured organization", with our prior written approval, that directly relate to the "insured's efforts to prevent or terminate an "extortion threat".

14. "Damages" means a monetary judgment, award or settlement. The term "damages" shall not include or mean:
    A. future profits, restitution, disgorgement of unjust enrichment or profits by an insured, or the costs of complying with orders granting injunctive or equitable relief;
    B. return or offset of fees, charges, or commissions charged by or owed to an "insured' for goods or services already provided or contracted to be provided;
    C. taxes or loss of tax benefits;
    D. fines, sanctions or penalties;
    E. punitive or exemplary damages, or any damages which are a multiple of compensatory damages, unless insurable by law in any applicable venue that most favors coverage for such punitive, exemplary or multiple damages;
    F. discounts, coupons, prizes, awards or other incentives offered to the insured's customers or clients;
    G. liquidated damages, but only to the extent that such damages exceed the amount for which the insured would have been liable in the absence of such liquidated damages agreement; or
    H. any amounts for which the insured is not liable, or for which there is no legal recourse against the insured.

15. "Data asset" means any software or electronic data that exists in computer systems and that is subject to regular back up procedures.

16. "Data protection loss" means the reasonable and necessary costs and expenses incurred by the "insured organization" to regain access to, replace, restore, reassemble or recollect any "data asset", or if any "data asset" cannot reasonably be accessed, replaced, restored, reassembled or recollected, then the actual reasonable and necessary costs and expenses incurred by the "insured organization" to reach this determination. "Data protection loss" shall not mean, and there shall be no coverage for:
    A. costs or expenses incurred by the "insured organization" to identify or remediate software program errors or vulnerabilities or update, replace, restore, assemble, reproduce, recollect or enhance a "data asset" or "computer systems" to a level beyond that which existed prior to the alteration, corruption, destruction, deletion or damage of such "data asset"'
    B. costs or expenses to research or develop any "data asset", including but not limited to trade secrets or other proprietary information;
    C. the monetary value of profits, royalties or lost market share related to a data asset, including but not limited to trade secrets or other proprietary information or any other amount pertaining to the value of the "data asset";
    D. loss arising out of any liability to any third party for whatever reason; or
    E. legal costs or legal expenses of any type.

17. "Denial of service attack" means a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users.

18. "Digital currency" means a type of digital currency that:
    A. requires cryptographic techniques to regulate the generation of units of currency and verify the transfer thereof;
    B. is both stored and transferred electronically; and
    C. operates independently of a central bank or other central authority.

19. "Employee" means:
    A. A natural person:
        i. while in the regular service of the "insured organization" in the ordinary course of its business; and
        ii. whom the "insured organization" has the right to direct and control while performing labor or service for the "insured organization"; and
        iii. who is compensated directly by the "insured organization" through salary, wages or commissions;
    B. a natural person who is directed and controlled by the "insured organization" while performing labor or service for the "insured organization" pursuant to a lease or other written contract to which the "insured organization" is a party;
    C. a natural person volunteer who is directed and controlled by the "insured organization" while performing labor or service for the "insured organization";
    D. a natural person who is a licensed attorney and who is acting as "of counsel" for and on behalf of the "insured organization", but only with respect to the performance of his or her duties on behalf of the "insured organization";
    E. a natural person who is a director, trustee, officer, administrator, "manager" or partner of the "insured organization", when performing acts coming within the scope of the usual duties of a director, trustee, officer, administrator, "manager" or partner; or
    F. a natural person who is:
        i. a trustee, officer, "employee", administrator, fiduciary or manager of any Employee Welfare or Pension Benefit Plan, as defined in Employee Retirement Income Security Act of 1974 and any amendments thereto ("ERISA"), which is or becomes solely sponsored by the "insured organization"; or
        ii. required to be bonded by Title 1 of ERISA.

20. "Extended reporting period" means the period of time after the end of the "policy period" for reporting a "claim" as set forth in the "Policy Declarations" and as provided in Section VII of this Policy.

21. "Extortion payment" means cash, "digital currency", marketable goods or services demanded to prevent or terminate an "extortion threat". If an "extortion payment" is made by or on behalf of the "insured organization" in "digital currency", payment by us shall be made in United States Dollars equal to the US Dollar-value of the "digital currency" at the time the "extortion payment" is made. For purposes of this paragraph, an "extortion payment" using "digital currency" shall be considered "made" at the time that such "digital currency" is first recorded in a public ledger of transactions for such "digital currency".

22. "Extortion threat" means a threat to:
    A. alter, destroy, damage, delete or corrupt any "data asset";
    B. prevent access to "computer systems" or a "data asset";
    C. perpetrate a theft or misuse of a "data asset" on "computer systems" through external access;
    D. introduce "malicious code" into "computer systems" or to third party computer systems from "computer systems"; or
    E. publicly disclose a "data asset", "personally identifiable information" or "third party information" that is obtained by "unauthorized access or us" to the "insured organization's" "computer systems",
    unless an "extortion payment" is received from or on behalf of the "insured organization".

23. "Extra expense" means reasonable and necessary expenses that are incurred by the "insured organization" during the "period of restoration" to minimize, reduce or avoid an "income loss", over and above those expenses the "insured organization" would have incurred had no interruption of "computer systems" occurred.

24. "Financial institution" means
    A. a bank, credit union, saving and loan association, trust company or other licensed financial service where the "insured organization" maintains a "transfer account"; or
    B. a securities broker-dealer, mutual fund, liquid assets fund or similar investment company where the "insured organization" maintains a "transfer account".

25. "Forensic expenses" means reasonable and necessary expenses incurred by the "insured organization" to investigate the source or cause of the failure of "computer security" to prevent a "security breach".

26. "Fraudulent instructions" means a fraudulent written instruction, electronic instruction (including email or web-based instruction) or telephone instruction provided by a person purporting to be a "vendor", "client", or an "authorized employee", that is intended to mislead an insured through the misrepresentation of a material fact that is relied upon in good faith by such insured.

27. "Funds transfer fraud" means fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions by a third party issued to a "financial institution" directing such institution to transfer, pay or deliver "money" or "securities" from any account maintained by the "insured organization" at such institution, without the "insured organization's" knowledge or consent.

28. "Income loss" means an amount equal to:
    A. the net profit or loss before interest and tax that the "insured organization" would have earned or incurred; and
    B. continuing normal operating expenses incurred by the "insured organization" (including payroll), but only to the extent that such operating expenses must necessarily continue during the "period of restoration" and such expenses would have been incurred by the "insured organization" had such interruption not occurred.

    In determining "income loss", due consideration shall be given to:
    A. the prior experience of the "insured organization's" business operations before the beginning of the "period of restoration";
    B. the probable business operations the "insured organization" could have performed had no actual and necessary interruption occurred as result of a failure of "computer security" to prevent a "security breach"; and
    C. the "insured organization's" ability to reasonably reduce or limit the interruption of "computer systems" or conduct its business operations by other means.

29. "Insured organization" means the "named insured" and any "subsidiaries" of the "named insured".

30. "Legal services" means fees charged by an attorney:
    A. to determine the applicability of and actions necessary for the "insured organization" to comply with "breach notice laws" due to an actual or reasonably suspected theft, loss or "unauthorized disclosure" of "personally identifiable information";
    B. to provide necessary legal advice to the "insured organization" in responding to actual or suspected theft, loss or "unauthorized disclosure" of "personally identifiable information";
    C. to advise the "insured organization" regarding the notification of relevant governmental entities of an actual or reasonably suspected theft, loss or "unauthorized disclosure" of "personally identifiable information"; and
    D. to advise the "insured organization" in responding to credit card system operating regulation requirements for any actual or suspected compromise of credit card data that is required to be reported to the "insured organization's" merchant bank under the terms of a "merchant services agreement"; however, "legal services" do not include fees incurred in any actual or threatened legal proceeding, arbitration or mediation, or any advice in responding to credit card system operating regulation in connection with an assessment of "PCI fines, expenses, and costs".

    "Legal services" will be provided in accordance with the terms and conditions set forth in this Policy and will be provided by an attorney from our panel selected by us in consultation with the "insured organization".

31. "Loss" means:
    A. "damages";
    B. "claims expenses";
    C. privacy breach response services;

D. "PCI fines, expenses and costs";
E. "cyber extortion loss";
F. "data protection loss";
G. "business interruption loss";
H. "penalties"; and
I. loss under **Section I – Insuring Agreements, 9. Fraudulent Instruction** and **10. Electronic Crime.**

32. "Malicious code" means any virus, Trojan horse, worm or any other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

33. "Management control" means:
A. owning, directly or indirectly, more than fifty percent (50%) of the outstanding securities, representing the present right to vote for the election of an entity's directors, members of the board of managers, management committee members or persons serving in a functionally equivalent role for such an entity operating or organization outside of the United States; or
B. having the right, pursuant to a written contract or bylaws, charter, operating agreement or similar documents of an entity to elect, appoint or designate a majority of:
i. the Board of Directors of a corporation;
ii. the Management Committee of a joint venture or partnership;
iii. the Management Board of a limited liability company; or
iv. persons serving in a functionally equivalent role for such an entity operating or organized outside of the United States.

34. "Manager" means manager of a limited liability company.

35. "Media material" means any information in electronic form, including words, sounds, numbers, images, or graphics and shall include advertising, video, streaming content, web-casting, online forums, bulletin boards and chat room content, but does not mean computer software or the actual goods, products or services described, illustrated or displayed in such "media material".

36. "Merchant services agreement" means any agreement between an insured and a financial institution, credit/debit company, credit/debit card processor or independent service operator enabling an insured to accept credit card, debit card, prepaid card, or other payment cards for payments or donations.

37. "Money" means:
A. currency, coins or bank notes in current use and having a face value; and
B. traveler's checks, register checks or money orders held for sale to the public.

38. "Named insured" means the individual, partnership, entity or corporation designated as such in the declarations of the policy.

39. "Notification services" means:
A. notification by first class mail or e-mail to United States, Canadian or Mexican residents; and
B. notification by first class mail or e-mail to individuals residing outside the United States, Canada or Mexico, but only to the extent reasonably practicable.
"Notification services" will be provided by a service provider from our panel selected by us in consultation with the "insured organization".

40. "Notified individual" means an individual person to whom notice is given or attempted to be given under paragraph d. of **SECTION I – INSURING AGREEMENTS, 2. Privacy Breach Response Services** pursuant to a "breach notice law".

41. "Out-of-band authentication" means a method of challenge and response to the requestor of a transfer, payment or delivery of "money" or "securities" by an insured, via a method other than the original means of request and via contact information previously provided to the "named insured" prior to the request, to verify the authenticity or validity of the request.

42. "PCI fines, expenses and costs" means the direct monetary fines, penalties, reimbursements, fraud recoveries or assessments owed by the "insured organization" under the terms of a "merchant services agreement", but only where such fines, penalties, reimbursements, fraud recoveries or assessments result both from the "insured organization's" actual or alleged noncompliance with published Payment Card Industry (PCI) Data Security Standards and from a data breach caused by an incident, or reasonably suspected incident, described in paragraphs A. and B. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**; provided, that the term "PCI fines, expenses and costs" shall not include or mean any charge backs, interchangeable fees, discount fees or prospective service fees.

43. "Penalties" means:
    - **A.** any civil fine or punitive sum of money payable to a governmental entity that was imposed in a "regulatory proceeding" by any other federal, state, local or foreign governmental entity, in such entity's regulatory or official capacity; the insurability of "penalties" shall be in accordance with the law in the applicable venue that most favors coverage for such "penalties"; and
    - **B.** amounts which the insured is legally obligated to deposit in a fund as equitable relief for the payment of consumer claims due to an adverse judgment or settlement of a "regulatory proceeding"; but shall not include payments to charitable organizations or disposition of such funds other than for payment of consumer claims for losses caused by an event covered pursuant to paragraphs A., B., or C. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability**;
    - **C.** "Penalties" do not mean:
        - **i.** costs to remediate or improve "computer systems";
        - **ii.** costs to establish, implement, maintain, improve or remediate security or privacy practices, procedures, programs or policies;
        - **iii.** audit, assessment, compliance or reporting costs; or
        - **iv.** costs to protect the confidentiality, integrity and/or security of "personally identifiable information" from theft, loss or disclosure.

44. "Period of restoration" means the time period that:
    - **A.** begins after the expiration of the "waiting period" following the actual and necessary interruption of "computer systems" and
    - **B.** ends one hundred twenty (120) days after the actual and necessary interruption of "computer systems" ends (or would have ended with the exercise of due diligence and dispatch);

    provided that in no event shall the "period of restoration" mean a period of time greater than one hundred eighty (180) days; and provided further that restoration of "computer systems" will not end the "period of restoration" if such systems are actually and necessarily interrupted or suspended again within one hour of such restoration due to the same cause as the original interruption or suspension.

45. "Personally identifiable information" means:
    - **A.** information concerning the individual that constitutes nonpublic personal information as defined in the Gramm-Leach Bliley Act of 1999, as amended, and regulations issued pursuant to this Act;
    - **B.** medical or health care information concerning the individual, including protected health information as defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and regulations issued pursuant to this Act;
    - **C.** information concerning the individual that is defined as private personal information under statutes enacted to protect such information in foreign countries, for "claims" subject to the law of such jurisdiction;
    - **D.** information concerning the individual that is defined as private personal information under a "breach notice law";
    - **E.** education records as defined by the Family Educational Rights and Privacy Act which are directly related to an individual's attendance as a student; or
    - **F.** the individual's drivers' license or state identification number, social security number, unpublished telephone number, and credit, debit, or other financial account numbers in combination with associated security codes, access codes, passwords or pins; if such information allows an individual to be uniquely and reliably identified or contacted or allows access to the individual's financial account or medial record information.

    "Personally identifiable information" does not include publicly available information that is lawfully made available to the general public from government records.

46. "Policy Declarations" means the "Policy Declarations" attaching to this Policy for the current "policy period" listed in the "Policy Declarations".

47. "Policy period" means the period of time between the inception date and the effective date of "termination of coverage" and specifically excludes any optional "extended reporting period" or any prior policy period or renewal period.

48. "Privacy law" means a federal, state or foreign statute or regulation requiring the "insured organization" to protect the confidentiality and/or security of "personally identifiable information".

49. "Privacy policy" means the "insured organization's" public declaration of its policy for collection, use, disclosure, sharing, dissemination and correction or supplementation of, and access to "personally identifiable information".

50. "Property" means tangible property other than "money" or "securities" that has intrinsic value.

51. "Public relations and crisis management expenses" shall mean the following costs, approved in advance by us, which are directly related to mitigating harm to the "insured organization's" reputation or potential "loss" covered by this Policy resulting from an incident described in paragraphs A. and B. of **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** or from a "public relations event":

- **A.** costs incurred by a public relations or crisis management consultant;
- **B.** costs for media purchasing or for printing or mailing materials intended to inform the general public about the incident;
- **C.** for incidents or events in which notifications services are not otherwise provided pursuant to **SECTION I – INSURING AGREEMENTS, 1. Information Security and Privacy Liability** and **2. Privacy Breach Response Services**, costs to provide notifications and notices via e-mail or first class mail to affected individuals where such notifications are not required by law (voluntary notifications), including non-affected customers or patients of the "insured organization";
- **D.** costs to provide government mandated public notices related to breach events (including such notifications required under the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act;
- **E.** costs to provide services to restore healthcare records of "notified individuals" residing in the United States whose "personally identifiable information" was compromised as a result of theft, loss or "unauthorized disclosure"; and
- **F.** other costs approved in advance by us.

"Public relations and crisis management expenses" must be incurred no later than twelve (12) months following the reporting of such "claim" or breach event to us and, with respect to paragraphs a. and b. above, within ninety (90) days following the first publication of such "claim" or incident. If voluntary notifications are provided, e-mail notification will be provided in lieu of first class mail to the extent practicable.

52. "Public relations event" means the publication or imminent publication in a newspaper (or other general circulation print publication) or on radio, television or a publically accessible website of a covered "claim" or incident under this Policy.

53. "Regulatory proceeding" means a request for information, civil investigative demand or civil proceeding commenced by service of a complaint or similar proceeding brought by or on behalf of any federal, state, local or foreign governmental entity in such entity's regulatory or official capacity in connection with such proceeding.

54. "Related party" means the "insured organization" and any past, present or future employees, directors, officers, "managers", partners or natural person independent contractors of the "insured organization".

55. "Retention" means the Retention amount for each "claims" stated in the "Policy Declarations".

56. "Retroactive date" means the date shown as the "retroactive date" in the "Policy Declarations".

57. "Securities" mean negotiable and non-negotiable instruments or contracts representing either "money" or property.

58. "Security breach" means:

- **A.** "unauthorized access or use" of "computer systems", including "unauthorized access or use" resulting from the theft of a password from a "computer system" or from any insured;

B. A "denial of service attack" against "computer systems" or "computer systems" that are not owned, operated or controlled by an insured; or

C. infection of "computer systems" by "malicious code" or transmission of "malicious code" from "computer systems".

A series of continuing "security breaches", related or repeated "security breaches", or multiple "security breaches" resulting from a continuing failure of "computer security" shall be considered a single "security breach" and be deemed to have occurred at the time of the first such "security breach".

59. "Subsidiary" means any corporation, limited liability company, joint venture or partnership while the "named insured" has "management control" over such entity, if the "named insured":

A. had "management control" over such entity on the inception date of this Policy or such entity was an insured under a Policy issued by us of which this Policy is a renewal;

B. acquires "management control" after the inception date of this Policy provided the revenues of the entity do not exceed fifteen percent (15%) of the "named insured's" annual revenues for the four quarterly periods directly preceding inception of this Policy; or

C. provided that this coverage only provides coverage for acts, errors, omissions, incidents or events that take place while the "named insured" has "management control" over such entity.

60. "Third party information" means any trade secret, data, design, interpretation, forecast, formula, method, practice, credit or debit card magnetic strip information, process, record, report or other item of information of a third party not insured under this Policy which is not available to the general public and is provided to the insured subject to a mutually executed written confidentiality agreement or which the "insured organization" is legally required to maintain in confidence; however, "third party information" shall not include "personally identifiable information".

61. "Transfer account" means an account maintained by the "insured organization" at a "financial institution" from which the "insured organization" can initiate the transfer, payment or delivery of "money" or "securities". "Unauthorized access or use" means the gaining of access to or use of "computer systems" by an unauthorized person or persons or the use of "computer systems" in an unauthorized manner.

62. "Unauthorized disclosure" means the disclosure of (including disclosure resulting from phishing) or access to information in a manner that is not authorized by the "insured organization" and is without knowledge of, consent, or acquiescence of any member of the "control group".

63. "Vendor" means any entity or natural person that provides goods or services to the insured pursuant to a written agreement.

64. "Waiting period" means the period of time beginning when the actual and necessary interruption of "computer systems" caused directly by a failure of "computer security" to prevent a "security breach" begins and expiring after the elapse of the number of hours set forth in the "Policy Declarations". A "waiting period" shall apply to each "period of restoration".

EXHIBITS LIST

DATA INTRUSION

Article on State Security Breach notifications

Idaho: Disclosure of Breach

Idaho: Penalties

Washington: Disclosure and Penalty provisions.

RANSOMWARE

Ransomware prevention advice

INSURANCE

ALPS POLICY

PREVENTION ADVICE

WannaCry additional prevention advice

1. Disable smb v1, this prevents Wannacry from spreading within your network.
2. Install the Microsoft patches, this also prevents Wannacry from spreading within your network. For more information click **here**.

How to prevent a ransomware attack?

1. Back-up! Back-up! Back-up! Have a recovery system in place so a ransomware infection can't destroy your personal data forever. It's best to create two back-up copies: one to be stored in the cloud (remember to use a service that makes an automatic backup of your files) and one to store physically (portable hard drive, thumb drive, extra laptop, etc.). Disconnect these from your computer when you are done. Your back up copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.
2. Use robust antivirus software to protect your system from ransomware. Do not switch off the 'heuristic functions' as these help the solution to catch samples of ransomware that have not yet been formally detected.
3. Keep all the software on your computer up to date. When your operating system (OS) or applications release a new version, install it. And if the software offers the option of automatic updating, take it.
4. Trust no one. Literally. Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues or an **online gaming** partner. Never open attachments in emails from someone you don't know. Cybercriminals often distribute fake email messages that look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.
5. Enable the 'Show file extensions' option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files. Stay away from file extensions like '.exe', '.vbs' and '.scr'. Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).
6. If you discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) – this will prevent the infection from spreading.

** The general advice is not to pay the ransom. By sending your money to cybercriminals you'll only confirm that ransomware works, and there's no guarantee you'll get the decryption key you need in return.*