\POLICY NUMBER:

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

CYBERSURANCE - PRIVACY AND SECURITY BREACH COVERAGE

SCHEDULE*

I. Effective Date:
(If no date entered, coverage is effective from policy inception.)

Additional Premium $_____

Limit of Liability	**$**			
Deductible	**$**			
Retroactive Date				
Claim Expenses	**Inside The Limit of Liability**	☐	**Outside The Limit of Liability**	☐
Payment Card Industry Fines And Penalties Revised Limit	**$**			

*Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

The changes described herein apply only with respect to this Cybersurance - Privacy And Security Breach Coverage endorsement. All provisions of the Policy apply unless modified by this endorsement.

With respect to the insurance afforded by this endorsement, the Limit of Liability and Deductible shown in the Schedule above apply in lieu of, not in addition to, the Limits of Liability and Deductible stated in the policy Declarations.

If the Schedule above shows that Claim Expenses are Inside the Limit of Liability, the coverage provided by this endorsement applies on a defense within limits basis. Any "claim expense" paid under this coverage will reduce the available Limit of Liability and may exhaust it completely.

II. In consideration of the additional premium shown above or in the Declarations, it is agreed that the insurance provided under **Section II - Coverage** is amended to include the following supplemental coverages:

A. Privacy Breach Liability Coverage

We will pay for all "loss" resulting from a "privacy breach" to which this insurance applies resulting from a "claim" first made against you during the "policy period", or any Extended Reporting Period provided, for an actual or alleged "privacy breach" which took place on or after the Retroactive Date, if any, shown in the Schedule.

B. Security Breach Liability Coverage

We will pay for all "loss" resulting from a "security breach" to which this insurance applies resulting from a "claim" first made against you during the "policy period", or any Extended Reporting Period provided, for an actual or alleged "security breach" which took place on or after the Retroactive Date, if any, shown in the Schedule that results in a "covered event".

C. Breach Notice Response Services Coverage

We will provide you with "breach notice response services" for a "privacy breach" covered under Section **II. A. - Privacy Breach Liability Coverage** or a "security breach" covered under Section **II. B. - Security Breach Liability Coverage** above that requires you to comply with any "breach notice laws".

D. Regulatory Response And Penalties Coverage

We will pay:

(1) "Claim expenses" required to evaluate or respond to a "claim" from any state or federal regulatory agency or other government agency; and

(2) Fines or penalties imposed by law;

due to or resulting from an actual or alleged "privacy breach" or "security breach".

Any "claim" under this Supplemental Coverage must first be made against you during the "policy period" or any Extended Reporting Period provided.

You agree to the use of an attorney retained by us, or hired by you with our written consent.

The most we will pay under this Supplemental Coverage is $25,000 per "policy period".

The most we will pay under this Supplemental Coverage during any Optional Extended Reported Period provided is $25,000.

The $25,000 limit provided by this Supplemental Coverage is part of and not in addition to the Limit of Liability shown in the Schedule.

Part **1.** under the "loss" definition does not apply to this Supplemental Coverage.

Exclusion **M.** does not apply to this Supplemental Coverage.

E. Payment Card Industry Fines And Penalties

We will pay for PCI fines or penalties stipulated in a written contract that you are required to pay because of your failure to comply with Payment Card Industry Data Security Standards (PCIDSS) for the handling of information in connection with payment card transactions.

Any "claim" under this Supplemental Coverage must first be made against you during the "policy period" or any Extended Reporting Period provided.

Unless a Revised Limit is shown in the Schedule, the most we will pay under this Supplemental Coverage is $10,000 per "policy period".

Unless a Revised Limit is shown in the Schedule, the most we will pay under this Supplemental Coverage during any Optional Extended Reported Period provided is $10,000.

The limit provided by this Supplemental Coverage is part of and not in addition to the Limit of Liability shown in the Schedule.

Any exclusion for amounts due under the terms of any contract in the Coverage Form to which this endorsement is attached does not apply to this Supplemental Coverage.

Part **1.** under the "loss" definition does not apply to this Supplemental Coverage.

You agree to use due diligence to prevent and mitigate any fines or penalties covered under this Supplemental Coverage. This includes, but is not limited to, making reasonable efforts to require your vendors, financial institutions, credit or debit card companies, credit or debit card processors, or other independent operators you use to accept payment, comply with reasonable and industry-accepted standards and protocols for protecting transactions, such as processing credit card, debit card and check payments.

F. RansomWare Coverage

We will provide you with "ransomware support services" if "your computer system" is held hostage by "ransomware" and you receive a ransom demand during the "policy period" or any Extended Reporting Period provided.

"Ransomware support services" means assistance provided to you if "your computer system" becomes infected with "ransomware". These services will be performed by a computer consultant who will attempt to free "your computer system" of the "ransomware" and regain access and restore system functionality. The assistance may be over the phone or in person. If it is not possible to free "your computer system" of "ransomware", the consultant can, at your request, assist you in restoring "your computer system" with a previously made backup of "your computer system", provided one is available.

"Ransomware" means any type of "malicious code" that is used to extort money by:

a. Locking down a computer system and restricting access to it; or

b. Encrypting some or all of a computer system's data files.

You agree to the use of a computer consultant retained by us, or hired by you with our written consent.

The most we will pay under this Supplemental Coverage is $50,000 per "policy period".

The most we will pay under this Supplemental Coverage during any Optional Extended Reported Period provided is $50,000.

The $50,000 limit provided by this Supplemental Coverage is part of and not in addition to the Limit of Liability shown in the Schedule.

This Supplemental Coverage does not apply to payment of any ransom demand.

III. Interrelated Events

Regardless of the number of insureds, "claims", or "suits", all "interrelated events" shall be considered a single "claim" and shall be deemed to have been made at the time the first of those "claims" is made against any insured. Only the Limit of Liability in effect on the date the first "claim" is made will apply to all "interrelated events". Only one Deductible will apply to all "interrelated events".

IV. Defense and Settlement of Claims

We will have the right and duty to defend the insured against any "claim" seeking "loss" to which this insurance applies even if the allegations of the "suit" are groundless, false or fraudulent. However, we will have no duty to defend the insured against any "claim" seeking "loss" to which this insurance does not apply. We may at our discretion:

A. Investigate any "claim"; and

B. Settle any "claim" which may result, provided:

1. We have your written consent to settle; and

2. The settlement is within the applicable Limit of Liability.

The amounts we will pay under this endorsement are limited as described in Section **VI.** below.

Our right and duty to defend end when we have used up the applicable Limit of Liability. Once the Limit of Liability shown in the Schedule above is exhausted, we will have no further obligation to pay "loss", "claim expense", "breach notice response services", or to undertake or continue the defense of any "claim". We will have the right to withdraw from the further defense of any "claim" under this coverage by tendering control of the defense to you. You will also be responsible for providing notification and "credit monitoring services" to "impacted individuals" and may continue to utilize any vendors recommended by us to provide such services.

V. Exclusions

The following exclusions replace and supersede those under **Section III - Exclusions** in the policy:

This insurance does not apply to any "privacy breach", "security breach", "claim" or "suit":

A. Alleging or arising out of any willful, deliberate, malicious, fraudulent, dishonest or criminal act, error or omission by an insured, or any intentional or knowing violation of law, or intentional "security breach" or "privacy breach" by an insured. This exclusion does not apply to "claim expense" incurred in defending an insured against any such "suit", but we will have no obligation to pay any "loss" for such conduct. However, if a court of competent jurisdiction or arbitrator determines that the insured's conduct was willful, deliberate, malicious, fraudulent, dishonest or criminal, we will have the right to recover all "claim expense" we incurred to defend those insureds found to have committed such conduct.

The insured shall reimburse us for all "claim expense" incurred defending the "suit" and we shall have no further liability for "claim expense". Such conduct shall not be imputed to the Named Insured if it occurs without the participation, knowledge, consent or acquiescence of any "management personnel".

B. Brought by an entity which:

1. You own or partly own, operate, manage or in which you have an ownership interest in excess of 15%, or in which you are an officer or director, except this provision will not apply to a "suit" that employee data is the subject of a "privacy breach" or violation of a "privacy regulation"; or

2. Wholly or partly owns, operates, controls or manages you.

C. Alleging or arising out of any "bodily injury" or "property damage".

D. Alleging or arising out of your insolvency, financial impairment or bankruptcy.

E. Alleging or arising out of any "suit", act, error, omission, circumstance, "privacy breach", "security breach", or potential "suit" reported to a prior insurer.

F. Alleging or arising out of any act, error, omission, circumstance, vulnerability, "privacy breach" or "security breach" if prior to the inception date of this endorsement, you knew, or reasonably could have foreseen, that such act, error, omission, circumstance, vulnerability, "privacy breach" or "security breach" might form the basis of a "claim" or potential "claim".

G. Alleging or arising out of any contractual liability or obligation, including without limitation, any liability assumed under contract, or alleging or arising out of or resulting from breach of contract or agreement, in either oral or written, including without limitation, any breach of express warranty or guarantee.

H. Alleging or arising out of any violation, misappropriation or infringement of any copyright, trademark, patent or other intellectual property right, or any copying, infringement, misappropriation, display, disclosure, publication or misappropriation of any trade secret.

I. Due to any actual or alleged electrical or mechanical breakdown, failure or interruption, disturbance, surge, spike, brownout or blackout; or outages to gas, water, telephone, cable satellite, telecommunications or other infrastructure comprising or supporting the Internet including service provided by the Internet service provider that hosts your website.

J. Alleging or arising out of any fire, smoke, explosion, lightning, wind, flood, surface water, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God or any other physical event, however caused.

K. Alleging or arising out of any 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.

L. Alleging or arising out of any:

1. War, invasion, acts of foreign enemies, hostilities or warlike operations (whether war be declared or not), civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, military or usurped power; or

2. Any act of terrorism.

For the purpose of this exclusion an act of terrorism means an act, including but not limited to the use of force or violence and/or the threat thereof, of any person or group(s) of persons, whether acting alone or on behalf of or in connection with any organization(s) or government(s), committed for political, religious, ideological or similar purposes including the intention to influence any government and/or to put the public, or any section of the public, in fear.

We also exclude loss, damage, cost or expense of whatsoever nature directly or indirectly caused by, resulting from or in connection with any action taken in controlling, preventing, suppressing or in any way relating to **1.** and/or **2.** above.

M. Brought by or on behalf of the Federal Trade Commission, Department of Health and Human Services, Office of Civil Rights, the Federal Communications Commission, or any other state, federal, local or foreign governmental entity, in such entity's regulatory or official capacity.

N. Alleging or arising out of any of the following:

1. Trading losses, trading liabilities or change in value of accounts; any loss, transfer or theft of monies, securities or tangible property of others in your care, custody or control; or

2. The monetary value of any transactions or electronic fund transfers by you or on your behalf which is lost, diminished, or damaged during transfer from, into or between accounts.

O. Made by one insured against another insured. However, this exclusion does not apply to a "suit" brought against you by your employee resulting from a "privacy breach" that is otherwise covered under Section **II. A. - Privacy Breach Liability Coverage** above.

P. Alleging or arising out of any wrongful employment practice, including, but not limited to harassment, hostile work environment, wrongful dismissal, discharge or termination, retaliation, wrongful disciplinary action, deprivation of career opportunity, failure to employ or promote, inadequate work place policies or procedures, or negligent evaluation of employees. However, this exclusion does not apply to any "claim" or "suit" resulting from a "privacy breach" that is otherwise covered.

Q. Alleging or arising out of any act, error or omission or breach of duty by any "management personnel" in the discharge of their duties if the "claim" or "suit" is brought by you or any of your principals, directors or officers, stockholders, members or employees in their capacity as such.

R. Alleging or arising out of the:

1. Unauthorized collection or acquisition of "personally identifiable information" by you, on your behalf, or with your consent or cooperation; or

2. 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".

S. Alleging or arising out of the:

1. Distribution of unsolicited email, direct mail or facsimiles, wire tapping, audio or video recording, or telemarketing by you or a third party on your behalf; or

2. Violation of any federal, state or local statute, ordinance or regulation that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information.

T. Alleging or arising out of your activities as a trustee, partner, officer, director or employee of any employee trust, charitable organization, corporation, company or business other than the Named Insured shown in the Schedule.

U. Alleging or arising out of any false, deceptive or unfair trade practice or violation of any consumer protection laws.

V. Alleging or arising out of any of the following:

1. Any violation of the Organized Crime Control Act of 1970 (commonly known as Racketeer Influenced and Corrupt Organizations Act or RICO), as amended, or any regulation promulgated thereunder or any similar federal law or legislation, or law or legislation of any state, province or other jurisdiction similar to the foregoing, whether such law is statutory, regulatory or common law;

2. Any 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, any state or provincial blue sky or securities law, any other federal securities law or legislation, or any other similar law or legislation of any state, province or other jurisdiction, or any amendment to the above laws, or any violation of any order, ruling or regulation issued pursuant to the above laws;

3. Any violation of the Fair Labor Standards Act of 1938, the National Labor Relations Act, the Worker Adjustment and Retraining Act of 1988, the Certified Omnibus Budget Reconciliation Act of 1985, the Occupational Safety and Health Act of 1970,

or any similar law or legislation of any state, province or other jurisdiction, or any amendment to the above law or legislation, or any violation of any order, ruling or regulation issued pursuant to the above laws or legislation;

4. Any breach of fiduciary duty, responsibility, or obligation in connection with any employee benefit or pension plan, including violation of the responsibilities, obligations or duties imposed upon fiduciaries by the Employee Retirement Income Security Act of 1974 as amended;

5. Any violation of any local, state or federal laws concerning antitrust or restraint of trade, or any false, deceptive or misleading advertising, or any violation of the Sherman Antitrust Act, the Clayton Act, or the Robinson-Patman Act, as amended; or

6. The knowing offshore movement, storage, processing or outsourcing of data to a legal jurisdiction outside of the United States and its Territories by you or a third party on your behalf.

VI. Limit of Liability

A. The Limit of Liability shown in the Schedule and the provisions below determine the most we will pay regardless of the number of:

1. Insureds;

2. "Claims" made or "suits" brought;

3. Persons or organizations making "claims"; or

4. "Privacy breaches" or "security breaches".

B. The Limit of Liability shown in the Schedule is the most we will pay for the sum of all "loss", "claim expense"* and "breach notice response services" covered by this endorsement.

*If the Schedule above shows that Claim Expenses are Inside The Limit of Liability.

C. The Limit of Liability for this coverage applies separately to each consecutive annual period and to any remaining period of less than 12 months, starting with the beginning of the "policy period" shown in the Declarations, unless the "policy period" is extended after issuance for an additional period of less than 12 months. In that case, the Limit of Liability for this coverage will be increased in proportion to any policy extension provided.

D. The Limit of Liability applies in excess of the Deductible shown in the Schedule. The Deductible applies to payments for "loss", "claim expense"* and "breach notice response services" covered by this endorsement. We may pay any part or all of the Deductible to settle or defend a "claim" or "suit". You agree to promptly reimburse us for any payments applicable to your Deductible.

*If the Schedule above shows that Claim Expenses are Inside The Limit of Liability.

VII. Conditions

The following changes apply to the **Conditions** Section:

A. The following replaces **Duties In The Event Of Wrongful Act, Claim Or Suit:**

Duties In The Event Of Privacy Breach, Security Breach, Claim Or Suit

1. You must provide written notice to us as soon as practicable of any "privacy breach", "security breach", "claim" or "suit". To the extent possible, notice should include:

a. The circumstances surrounding the "privacy breach" or "security breach" including how, when, and where it took place;

b. The names and addresses of persons involved and any witnesses;

c. The nature of the harm resulting from the "privacy breach" or "security breach";

d. The date the "claim" or "suit" was received; and

e. An indication of the number of individuals that may be impacted, the type of information involved, and the actions taken to mitigate or contain the "loss", "privacy breach" or "security breach".

2. You and any other involved insured must:

a. Authorize us to obtain records and other information;

b. Cooperate with us in the investigation, settlement or defense of the "claim", "suit", "privacy breach" or "security breach";

c. Assist us, upon our request, in the enforcement of any right against any person or organization which may be liable to an insured because of "loss" to which this insurance may also apply; and

d. Provide us with a copy of or link to your relevant "privacy policy" and information security policy if applicable.

3. No insured will, except at that insured's own cost, voluntarily make a payment, assume any obligation, or incur any expense without our consent.

4. It is a condition precedent to coverage under this endorsement that you obtain our written consent before you admit liability, make any payment, assume any obligation, incur any expense, enter into any settlement, stipulate to any judgment or award, agreement or other means of disposing of any "claim" or any portion of any "claim".

B. The following Conditions are added:

1. Computer System Protection

a. It is a condition precedent to coverage under this endorsement that at all times during the "policy period" you or your independent contractor shall:

(1) Maintain anti-virus software on any computer that is part of "your computer system" and routinely update the protection as reasonably necessary;

(2) Maintain firewalls on any computer that is part of "your computer system" and connected to the internet; and

(3) Take reasonable security precautions when processing, storing, or transmitting credit card payment data or "personally identifiable information".

b. It is a condition precedent to coverage under this endorsement for any "mobile storage device" that the "mobile storage device" is subject to regular strong encryption processes and protected by reasonable access controls to prevent unauthorized access to such hardware.

2. Reimbursement

In the event of a determination that there is no coverage under this endorsement, you agree to reimburse us for any and all "loss" and "claim expense" that we paid for any "suit" or portion of "suit" that was determined not to be covered.

VIII. Additional Services

The following **Additional Services** are available to you and do not affect the Limit of Liability:

A. Privacy Breach Management Services

In the event of a possible or actual "privacy breach" that may require you to comply with any "breach notice laws", we will provide you with "privacy breach management services" performed by the breach services consultants of our choice. The possible or actual "privacy breach" must be reported to us within ten (10) days of suspicion of or actual discovery of facts revealing a potential or actual "privacy breach" has occurred.

"Privacy breach management services" are available as needed for any one "privacy breach" for up to 12 consecutive months from the inception of the service. "Privacy breach management services" are available to you regardless of whether or not you have actually suffered a "privacy breach" and whether or not an actual "suit" under this endorsement results.

B. Identity Restoration Case Management Services

In the event of a "privacy breach" that requires you to comply with any "breach notice laws", we will provide "identity restoration case management services" performed by a Fraud Specialist.

"Identity restoration case management services" are available so long as any "identity fraud" related activity is first discovered by the "impacted individual" following a "covered event" under this endorsement.

"Identity restoration case management services" are available as needed for any "identity fraud" for up to 12 consecutive months from the inception of the service.

"Identity restoration case management services" are provided without regard to whether the person or persons committing the "identity fraud" are identified so long as the "impacted individual" is willing to complete a fraud victim affidavit and file a police report or incident report concerning the "identity fraud".

C. Service Definitions

1. "Account takeover" means the takeover by a third party of one or more existing deposit accounts, credit card accounts, debit card accounts, ATM cards, or lines of credit in the name of an "impacted individual".

2. "Fraud specialist" means an expert who will assist in resolving the fraudulent use, or suspected fraudulent use, of personal information and to restore it to pre-incident status to the extent possible and feasible under the law. This assistance may include contacting credit reporting agencies, credit grantors, collection agencies and government agencies or other activities needed to restore the identity information of the "impacted individual".

3. "Identity fraud" means and includes any fraudulent activity associated with an "account takeover" or "identity theft" suffered by an "impacted individual".

4. "Identity restoration case management services" means assistance to an "impacted individual" by a "fraud specialist" who will work on a one-on-one basis and provide help and guidance specific to the "impacted individual's" classification as an account takeover or identity theft victim.

5. "Identity theft" means a fraud committed or attempted by a third party using the identifying information of another person without authority and resulting in the creation of one or more new accounts, or a new identity in public records (such as a driver's license) or elsewhere.

6. "Privacy breach management services" means those services provided to you including:

a. Proactive Breach Preparation Services - Tools, educational material or information that can be used to instruct staff and prevent and prepare for a "privacy breach".

b. Reactive Breach Response Services - We will assist you with the handling and management of a "privacy breach". Such assistance may include guidance about best practices, documentation, or the overall process of responding to the "privacy breach". We may also assign breach services consultants to work directly with your breach management team, management or legal counsel.

c. Computer and Network Forensic Evaluation Consulting Services - We will provide general consulting on technical aspects of the "privacy breach" including assistance with determining if and what type of specific computer and network forensics you should undertake.

Computer and Network Forensic Evaluation Consulting Services does not include the actual performance of digital forensic services on "your computer systems" or networks and do not include suggestions or consulting regarding corrective actions to be taken by you to address inadequacies in "your computer system's" or network's security.

IX. Definitions

The following changes apply to Section **I** - Definitions:

A. "Claim expense" is replaced by the following:

"Claim expense" means only those reasonable legal fees, costs or expenses incurred by us or you with our prior written consent, to defend or investigate a "claim" or "suit". "Claim expense" does not include any salaries, overhead, lost productivity, or other internal costs, expenses or charges you incur; costs or expenses for mitigation of a "privacy breach" or "security breach"; the costs or expenses for or arising out of any security or privacy measures, controls, policies, procedures, assessments or audits; or the costs or expenses of any investigation of or compliance with any "breach notice law".

B. "Loss" is replaced by the following:

"Loss" means any amount which an insured becomes legally obligated to pay as compensatory damages arising out of any "claim" to which this insurance applies and shall include judgments and settlements. "Loss" shall not include:

1. Fines or penalties imposed by law;

2. Taxes;

3. Punitive or exemplary damages or any damages that are multiples of any other damages assessed against an insured;

4. Equitable relief, injunctive relief, declarative relief or any other relief or recovery other than monetary amounts; or

5. Matters which may be deemed uninsurable under the law pursuant to which the policy shall be construed.

C. The following definitions are added:

1. "Breach notice legal and forensic expenses" means:

a. Fees incurred for the services of a third party computer forensics professional to conduct an investigation to identify whether data containing "personally identifiable information" was accessed by an unauthorized person as a result of a covered "privacy breach"; and

b. Attorney fees for an outside attorney to determine whether any "breach notice laws" apply and the obligations of such applicable laws, and assist you to comply with such laws, including but not limited to drafting notice letters to "impacted individuals".

2. "Breach notice law" means any governmental statute or regulation that requires an organization to provide notice to those individuals whose "personally identifiable information" was actually, or was reasonably believed to have been, accessed by an unauthorized third party.

3. "Breach notice response services" means any of the following expenses incurred by us, or by you with our prior written consent, with respect to "impacted individuals":

a. "Breach notice legal and forensic expenses";

b. "Notice fulfillment services"; and

c. "Credit monitoring services".

4. "Covered event" means any of the following:
   a. Unauthorized access to, or unauthorized use of, "your computer system";
   b. Physical theft or loss of a "data storage device" that results in unauthorized access to "personally identifiable information", including a "data storage device" that is a laptop computer;
   c. Transmission of "malicious code" from "your computer system" to a third party's computer system;
   d. "Denial of service attack" targeted at "your computer system" or launched from "your computer system" against a third party's computer system; or
   e. An intentional and malicious theft, copying, alteration, destruction, deletion or damage to data stored on or transmitted within "your computer system", including without limitation "personally identifiable information" stored electronically on "your computer system".
5. "Credit monitoring services" means twelve (12) months of "credit monitoring services" provided to each "impacted individual", but only if such individual actually enrolls for and redeems such services. This endorsement does not cover any expenses related to or arising out of "credit monitoring services" where an "impacted individual" has not enrolled for and redeemed such services. "Credit monitoring services" notify an affected individual by e-mail when there is any change or suspicious activity on a credit record on file with a credit reporting agency.
6. "Data storage device" means any:
   a. "Mobile storage device"; or
   b. Computer hardware on which "personally identifiable information" is stored that is not a "mobile storage device", and that is protected by reasonable access controls to prevent unauthorized access to such hardware, including without limitation internal hard-drives, desktop computers, back-up tapes and servers.

   "Data storage device" however does not mean or include any phone devices (including without limitation any smart phone) or any device or equipment leased to you or leased or sold by you.
7. "Denial of service attack" means an intentional and malicious attack by a third party intended by such to block or prevent access to a computer system.
8. "Impacted individual" means an individual whose "personally identifiable information" was compromised as a result of a "privacy breach".
9. "Interrelated events" means "claims" for "privacy breaches" or "security breaches" which arise out of and have as a common basis:
   a. Related circumstances, situations, events, transactions or facts;
   b. A series of related circumstances, situations, events, transactions or facts; or
   c. A common pattern of conduct.
10. "Malicious code" means any virus, Trojan, worm or other similar malicious software program, code or script (including without limitation any of the foregoing that are specifically targeted or generally targeted at multiple computers or networks) intentionally designed to infect and harm a computer system, harm data on a computer system, or steal data from a computer system.
11. "Management personnel" means your officers, directors, risk managers, partners, managing members of an LLC, or staff attorney (including without limitation any CIO, CSO, CEO, COO, GC, CISO, or CFO), or any individual in a substantially similar position, or having substantially similar responsibilities, as the foregoing, irrespective of the exact title.
12. "Mobile storage device" means any laptop computer, external hard-drive, thumb-drive, non-phone PDAs or flash storage device on which "personally identifiable information" is stored.
13. "Notice fulfillment services" means fulfillment services to provide notice to "impacted individuals" as required under applicable "breach notice laws", including printing services, email notice, media notice, mailing services and postage.

14. "Personally identifiable information" means any of the following information, in electronic form or paper media, in your care, custody or control, or the care, custody or control of a third party that provides services on your behalf pursuant to a written agreement which fully indemnifies you for any claims, loss and costs arising out of any unauthorized access or use of such information:

a. A person's first and last name, or first initial and last name in combination with: social security number, passport number or any other national identification number; driver's license number or any other state identification number; medical or healthcare data including protected health information; or any account number, credit or debit card number in combination with any required password or security code that would permit access to the financial account;

b. Non-public personal information as defined in any "privacy regulation"; or

c. An Internet Protocol (IP) address where utilizing reasonable knowledge means you can identify a specific individual with such IP address.

15. "Privacy breach" means any of the following:

a. Theft or loss of "personally identifiable information"; or

b. Your negligent failure to comply with that portion of your "privacy policy" explicitly:

(1) Allowing a person to access or correct his or her "personally identifiable information"; or

(2) Requiring the destruction or deletion of "personally identifiable information";

provided, however, that at the time of such failure you must have had in force an existing "privacy policy" addressing such issues described in **(1)** and **(2)** above.

16. "Privacy policy" means your written and publicly disclosed policies identifying your practices for the collection, use, disclosure, sharing, allowing of access to, and correction of "personally identifiable information".

17. "Privacy regulation" means any statute or regulation addressing the control, use or protection of "personally identifiable information".

18. "Security breach" means the inability and failure of your existing technical or physical security measures of "your computer system" to prevent unauthorized access to or unauthorized use of "your computer system".

19. "Your computer system" means any computer hardware, software or firmware, and components thereof including data stored thereon, that is:

a. Owned or leased by you and which is under your direct operational control; or

b. Under the direct operational control of an independent contractor or other third party that provides services on your behalf; provided that such independent contractor or other third party has agreed pursuant to a written contract with you to fully indemnify you for any claims, loss and costs arising out of any unauthorized access or use of such computer hardware, software or firmware, components and data.

"Your computer system" does not include any cloud service provider, or any data stored in or controlled in whole or in part by any cloud service provider.