Gallagher

BCS

Powered by LLOYD'S

# Cyber Insurance Quotation




# Frequently Asked Questions

Do you have any questions about your insurance? The frequently asked questions below are here to help you make an informed decision.

## What is Cyber Insurance?

"Cyber" insurance is insurance coverage specifically designed to protect a business or organization from a range of threats and incidents relating to a breach event including:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private
- Liability claims alleging invasion of privacy and/or copyright/trademark violations in a digital, online or social media environment
- Liability claims alleging failures of computer security that result in deletion/alteration of data, transmission of malicious code, denial of service, etc.
- Defense costs in State or Federal regulatory proceedings that involve violations of privacy law; and
- The provision of expert resources and monetary reimbursement to the Insured for the out-of-pocket (1st Party) expenses associated with the appropriate handling of the types of incidents listed above

The term "Cyber" implies coverage only for incidents that involve electronic hacking or online activities, when in fact this product is much broader, covering private data and communications in many different formats – paper, digital or otherwise.

## What does Privacy Liability (including Employee Privacy) cover?

The Privacy Liability aspect of the insuring agreement in our policy goes beyond providing liability protection for the Insured against the unauthorized release of Personally Identifiable Information (PII), Protected Health Information (PHI), and corporate confidential information of third parties and employees, like most popular "Data Breach" policies. Rather, our policy provides true Privacy protection in that the definition of **Privacy Breach** includes violations of a person's right to privacy, etc. Because information lost in every data breach may not fit State or Federal-specific definitions of PII or PHI, our policy broadens coverage to help fill these potentially costly gaps. This is a key provision that truly sets the BCS policy apart from others.

## What does Privacy Regulatory Claims Coverage cover?

The Privacy Regulatory Claims Coverage insuring agreement provides coverage for both legal defense and the resulting fines/penalties emanating from a **Regulatory Claim** made against the Insured, alleging a privacy breach or a violation of a Federal, State, local or foreign statute or regulation with respect to privacy regulations.

## Does this policy cover regulatory investigations and/or fines related to GDPR privacy violations?

The BCS cyber policy has always provided broad **Regulatory Claim** coverage that would contemplate defense and penalties associated with unintentional violations of domestic and foreign privacy statutes. In accordance with the implementation of the EU's General Data Protection Regulation, BCS added clarifying language to the policy form under the definitions of **Privacy Regulations** and **Private Information** to specifically reference coverage for GDPR by name (subject to policy terms and conditions). It is important to note that fines and penalties may not be insurable by law in certain U.S. States and in certain foreign countries, including some member countries of the European Union.

## Does this policy cover regulatory investigations and/or fines related to privacy violations of the California Consumer Privacy Act (CCPA) or the Biometric Information Privacy Act (BIPA) in Illinois?

As the nature and complexity of privacy laws continues to expand across not only the U.S., but the world, the BCS policy is well positioned to address these concerns, where insurable by law. Both the California Consumer Privacy Act and the Biometric Information Privacy Act are examples of the "future-proof" nature of coverage afforded under the policy's broad definition of **Privacy Regulations**. For instance, some insurers have issued endorsements to their policies to carve back coverage for CCPA in their anti-trust exclusions. The BCS policy has already contemplated this via carvebacks for **Regulatory Claims**, so no change of that nature is necessary. Further, some carriers have endorsed their forms to carve back coverage for CCPA in their Wrongful Collection or Gathering or Distribution of Information exclusion. No such exclusion exists in the BCS form, making an additional endorsement of this nature unnecessary. Lastly, with respect to covering the unlawful collection of, or protection of biometric information, the definition of **Private Information** in the BCS form is significantly broader than many competing forms, thus, information of this nature is inherently contemplated in the coverage.

## What does Security Breach Response Coverage cover?

This 1st Party coverage reimburses an Insured for costs incurred in the event of a security breach of personal, non-public information of their customers or employees. Examples include:

- The hiring of a public relations consultant to help avert or mitigate damage to the Insured's brand
- IT forensics, customer notification and 1st Party legal expenses to determine the Insured's obligations under applicable Privacy Regulations
- Credit monitoring expenses for affected customers for up to 12 months, and longer if circumstances require.

The BCS policy can also extend coverage even in instances where there is no legal duty to notify if the Insured feels that doing so will mitigate potential brand damage (such voluntary notification requires prior written consent).

## What does Security Liability cover?

The Security Liability insuring agreement provides coverage for the Insured for allegations of a **Security Wrongful Act**, including:

- The inability of a third-party, who is authorized to do so, to gain access to the Insured's computer systems
- The failure to prevent unauthorized access to or use of a computer system, and/or the failure to prevent false communications such as phishing that results in corruption, deletion of or damage to electronic data, theft of data and denial of service attacks against websites or computer systems of a third party
- Protects against liability associated with the Insured's failure to prevent transmission of malicious code from their **Computer System** to a third party's **Computer System**

## What does Multimedia Liability cover?

The Multimedia Liability insuring agreement provides broad coverage against allegations that include:

- Defamation, libel, slander, emotional distress, invasion of the right to privacy, copyright and other forms of intellectual property infringement (patent excluded) in the course of the Insured's communication of **Media Content** in electronic (website, social media, etc.) or non-electronic forms

Other Cyber insurance policies often limit this coverage to content posted to the Insured's website. Our policy extends what types of media are covered as well as the locations where this information resides.

## What does Cyber Extortion cover?

The Cyber Extortion insuring agreement provides:

- Expense and payments (including ransom payments if necessary) to a third party to avert potential damage threatened against the Insured such as the introduction of malicious code, system interruption, data corruption or destruction or dissemination of personal or confidential corporate information.
- Ramsomware is among the most reported types of cybersecurity incidents. Verizon's 2018 Data Breach Investigations Report (DBIR) indicated that ransomware is the most common type of malware, found in 39 percent of malware-related data breaches – double of the amount reported in last year's DBIR. Investigation and other expenses associated with ransomware events are contemplated under the **Cyber Extortion** insuring agreement. Additionally, Symantec's 2018 Internet Security Threat Report indicated that 2017 brought a 46% increase in new ransomware variants. Having the proper team in place to help you navigate the intricacies of a ransomware attack is critical and the BCS policy provides this through the **Cyber Extortion** coverage.

## What does Business Income and Digital Asset Restoration cover?

The Business Income and Digital Asset Restoration insuring agreement provides for lost earnings and expenses incurred because of a **Network Disruption**, or, an authorized third-party's inability to access a **Computer System** . The policy will also cover for lost business as a result of a loss of reputation caused by any failure or disruption to **Computer Systems**. **Restoration Costs** to restore or recreate digital (not hardware) assets to their pre-loss state are provided for as well. What's more, the definition of **Computer System** is broadened to include not only systems under the Insured's direct control, but also systems under the control of a **Service Provider** with whom the Insured contracts to hold or process their digital assets. Many competing Cyber insurance forms require that a **Security Breach** take place in order for Business Interruption coverage to respond. The BCS form is unique in that the definition of **Network Disruption** is extremely broad and includes any unplanned failure, interruption or degradation of the operation of your **Computer System** or the **Computer System** of a an IT service provider – whether it was caused by a **Security Breach** or otherwise. The BCS policy further differentiates itself by taking this expansion of coverage a step further. In addition to IT service providers, coverage for **Network Disruption** is provided (on a sub-limited basis) to **Outsourced Providers**, that is, any provider, other than an IT **Service Provider**, that provides services (other than IT services) for you, pursuant to a written contract. This expanded coverage is offered without the need for additional underwriting and is sometimes referred to as "Supply Chain Business Interruption"

## What is Systems Integrity Restoration coverage?

A sub-section of the **Business Income and Digital Asset Restoration** insuring agreement, **Systems Integrity Restoration Loss** provides a sub-limit for costs associated with replacement of an Insured's **Computer System** directly impacted by a **Security Compromise**.

## What is "PCI-DSS Assessment" coverage?

The Payment Card Industry Data Security Standard (PCI-DSS) was established in 2006 through a collaboration of the major credit card brands as a means of bringing standardized security best practices for the secure processing of credit card transactions. Merchants and service providers must adhere to certain goals and requirements in order to be "PCI Compliant," and certain specific agreements, may subject an Insured to an "assessment" for breach of such agreements. The AJG Cyber Policy responds to **PCI Assessments** as well as claims expenses in the wake of a breach involving cardholder information. Additionally, this coverage provides for expenses associated with a mandatory audit performed by a Qualified Security Assessor (QSA), certified by the PCI Security Standards Council, to show you are PCI DSS compliant, following a **Security Breach**.

## What is Cyber Deception coverage?

The **Cyber Deception** extension is purchased for an additional premium if the applicant is eligible. The extension provides coverage for the intentional misleading of the Applicant by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which is relied upon by the Applicant believing it to be genuine. This is commonly known as spear-phishing or social engineering", and, along with ransomware events, is among the most reported incidents to the BCS Cyber policy. Many Cyber policies offering this coverage require that the insured call back, or, attempt to verify the request's authenticity via a method other than the original means. In other words, if a request to transfer money to a different bank routing number is received via email, other Cyber policies may require that the person receiving the email attempt to verify the request also via telephone before authorizing the transfer of money. While the application process asks a question regarding controls in place for this, the BCS policy differentiates itself further by not requiring this of insureds in the policy wording. Additionally, this coverage provides for the loss of money from the Insured's account, or, the loss of money held on behalf of the Insured's customers or clients (aka funds held in escrow). The BCS policy does not presently offer **Cyber Deception** coverage to financial institutions or title agents.

## What is Telephone Hacking coverage?

**Telephone Hacking** coverage is included in the **Electronic Fraud** sub-section of the BCS policy. It provides a sub-limit of coverage for the intentional, unauthorized and fraudulent use of your **Telecommunications Services** (ie: telephone, fax, broadband or other data transmission services that you purchase from third parties) that results in unauthorized calls or unauthorized use of your bandwidth.

## What is Funds Transfer Fraud coverage?

**Funds Transfer Fraud** coverage is available in the **Electronic Fraud** sub-section of the BCS policy for insureds who are NOT classified as Financial Institutions (Financial Institutions includes Community, State or Credit Unions, as well as National Financial Institutions, Banks, etc.) or Title/Escrow/Settlement/Closing Agents or Agencies. For those organizations who are not in the Financial Institution or Title/Escrow/Settlement/Closing Agents or Agencies classifications, the coverage provides coverage for unauthorized electronic funds transfer, theft of your money or other financial assets from your bank by electronic means, theft of your money or other financial assets from your corporate credit cards by electronic means, or any fraudulent manipulation of electronic documentation while stored on your **Computer System**. This should not be confused with **Cyber Deception** coverage which requires a willful release of funds (not theft) based on a fraudulent instruction the insured believes to be true.

## What is Phishing coverage?

Coverage for **Phishing Loss** is available in the **Electronic Fraud** sub-section of the BCS policy. The coverage provides reimbursement to the Insured when they are unable to collect a receivable due to them because of a third party's impersonation of them via email or other electronic means. This is often experienced when the Insured's system is compromised and a fraudster sends out an invoice, purporting to come from the Insured, however, payment routing information is changed to divert funds to the fraudster who is executing the crime. As a result, customers pay over amounts owed to fraudulent accounts, instead of to the Insured's account, and the Insured is unable to collect the monies owed to them.

## What is Services Fraud Loss coverage?

**Services Fraud Loss** is provided in the **Electronic Fraud** sub-section of the BCS policy. "Cryptojacking" is an illegal activity on the rise whereby hackers infiltrate an Insured's system and utilize the computing power of the network they have taken over in order to mine digital currencies. This vast increase in the infiltrators' computing resources can lead to excessive bandwidth charges that the Insured could unknowingly incur as a result of the incident. **Services Fraud Loss** will also reimburse the Insured in the event their **Computer System** is taken over by a third party and they incur charges associated with the unauthorized use of Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Network-as-a-Service (Naas) or IP telephony.

## What is Reward Fund Loss coverage?

Also provided in the **Electronic Fraud** sub-section of the BCS policy, **Reward Fund Loss** provides reimbursement to the Insured (subject to prior underwriter consent) for monies they pay for information that leads to the arrest and conviction of any individuals committing or trying to commit an illegal act associated with a covered **Event** in the policy.

## What is Personal Financial Loss coverage?

**Personal Financial Loss**, provided in the **Electronic Fraud** sub-section of the BCS policy, reimburses senior executive officers of the Insured for theft of money or other financial assets from their personal bank account, or identity theft of a senior executive officer, resulting from a covered **Security Breach** or **Security Compromise**.

## What is Court Attendance Costs coverage?

Within the definition of **Claims Expenses**, **Court Attendance Costs** provides the Insured for reasonable sums they incur (with prior written agreement) to attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any covered **Claim** to which the Insured is entitled to a defense under the policy.

## What is Bodily Injury and Property Damage Liability coverage?

Typically, Cyber insurance policies carry absolute exclusions for **Bodily Injury** and **Property Damage** liability. The BCS policy provides a sub-limit of coverage for liabilities associated with **Bodily Injury** and/or **Property Damage** if resulting from a **Claim** described in the **Privacy Liability** or **Security Liability** insuring agreements.

## What is TCPA coverage?

The Telephone Consumer Protection Act (TCPA) is a law passed by the U.S. Congress in 1991 that amends the Communications Act of 1934. TCPA restricts telephone solicitations and the use of automated telephone equipment, automatic dialing systems, artificial or prerecorded voice messages, SMS text messages and other unsolicited means of communications. Most Cyber liability insurance policies carry a strict TCPA exclusion. The BCS policy provides a sub-limit of coverage for TCPA allegations and provides this coverage for both **Damages** and/or **Claims Expenses** – a clear differentiator in the marketplace.

### What is HIPAA Corrective Action Plan coverage?

Part of the **Regulatory Liability Claims Coverage** insuring agreement, **HIPAA Corrective Action Plan Costs** are costs the Insured is obligated to pay to meet any of the requirements specified within a HIPAA corrective action plan resulting from a **Regulatory Claim** covered by the policy. Examples of costs incurred in this regard could include conducting a risk analysis, implementing risk management plans to mitigate future risk, revision of policies and procedures related to the HIPAA Security Rule, implementation of training programs and more.

### What is Post Breach Response coverage?

Part of the **Breach Response Costs** definition, **Post Breach Response** provides the Insured a sub-limit of coverage (with prior consent, and utilizing pre-approved vendors) for costs incurred for the revision of an incident response plan, the completion of a network security audit, an information security risk assessment, and/or the implementation of a security awareness training program.

### What is Independent Consultant coverage?

An extension of the **Business Income Loss** definition, this coverage provides for necessary costs to retain an independent consultant to determine the amount of an Insured's **Business Income Loss**.

### What is Outsourced Provider coverage?

The policy provides a sub-limit of coverage for **Business Income Loss** resulting from a **Network Disruption** that occurs on an **Outsourced Provider's Computer System**. Outsourced Providers are businesses the Insured works with that perform services other than IT services, pursuant to a written contract. Also known as system failure coverage for "supply chain" partners, the coverage afforded under these terms is among the broadest in the industry.

### What is Computer Hardware coverage?

Found within the definition of **Restoration Costs**, the policy will provide for reasonable and necessary costs to install a more secure and efficient version of the Insured's **Computer System** up to 25% more than the cost would have been to replace the original model, subject to a sub-limit of coverage for hardware replacement.

### How is this policy better than other options in the marketplace?

As with any insurance policy, what sets our coverage apart lies in the definitions and exclusions in the policy. The BCS policy offers broader definitions of critical terms such as **Privacy Breach**, **Computer System**, and **Media Content**. Additionally, the BCS policy provides industry-leading coverage in the area of Business Interruption. These definitions, along with the absence of some industry-standard exclusions and a drastically streamlined application process, make this policy more comprehensive and easier to access than the typical Cyber policy available from traditional sources.

## Isn’t this already covered under most business insurance plans?

The short answer is "No". While liability coverage for data breach and privacy claims has been found in limited instances through General Liability, Commercial Crime and some D&O policies, these forms were not intended to respond to the modern threats posed in today's 24/7 information environment. Where coverage has been afforded in the past, carriers (and the ISO) are taking great measures to include exclusionary language in form updates that make clear their intentions of not covering these threats. Additionally, even if coverage can be found in rare instances through other policies, they lack the expert resources and critical 1st Party coverages that help mitigate the financial, operational and reputational damages a data breach can inflict on an organization.

## Are businesses required to carry this coverage?

While there is presently no law that requires a business or organization to carry Cyber Liability Insurance, there is a national trend in business contracts for proof of this coverage. In addition, the SEC and other regulatory bodies are encouraging disclosure of this coverage as a way of demonstrating sound information security risk management. Laws such as HIPAA-HITECH, GDPR and Gramm-Leach-Bliley and state-specific data breach laws are continually driving demand as requirements for notification in the wake of a data breach become more expensive, and expectations around the level of response by an impacted organization are increased.

## Do small businesses need this coverage?

A recent Ponemon Institute report uncovered that 50% of small and medium sized US businesses had suffered a data breach, with 55% suffering a cyber-attack, with the most prevalent attack being non-sophisticated phishing attempts. The US National Cyber Security Alliance has advised that 60% of small companies are out of business within 6 months after being hacked. While breaches involving public corporations and government entities garner the vast majority of headlines, it is the small business that can be most at risk. With lower information security budgets, limited personnel and greater system vulnerabilities, small businesses are increasingly at risk for a data breach. In the past, many small business owners in the SME space were reluctant to purchase Cyber liability insurance coverage because they did not see themselves as data rich targets. Today’s trends are showing that much of the data breach and ransomware attacks in today’s business environment are indiscriminant of industry or size. Random attacks distributed to thousands of unknown recipients with the hopes of snaring just a limited number have caused business owners of all sizes and descriptions to re-think their approach to this huge risk and purchase insurance to mitigate the effects.

## If e-commerce functions such as payment processing or data storage are outsourced, is this coverage still needed?

The responsibility to notify customers of a data breach or legal liabilities associated with protecting customer data, remain the responsibility of the Insured. Generally speaking, business relationships exist between Insureds and their customers, not their customers and the back-office vendors the Insured uses to assist them in their operations. Outsourcing business critical functions such as payment processing, data storage, website hosting, etc. can help insulate Insureds from risk, however, the contractual agreement wording between Insureds, their customers and the vendors with whom they do business will govern the extent to which liability is assigned in specific incidents.

## What is the cost of not buying the coverage and self-insuring a data breach?

The Ponemon Institute, a well-known research firm, publishes an annual "Cost of a Data Breach" report. In partnership with IBM, the 2017 report indicated that the average cost paid for each lost or stolen record is $148. These numbers are reflective of both the indirect expenses associated with a breach (time, effort and other organizational resources spent during the data breach resolution, customer churn, etc.), as well as direct expenses (customer notification, credit monitoring, forensics, hiring a law firm, etc.). The 2018 cost reflects a 6.4% increase over the 2017 report.

In 2018, The average total cost of a data breach, globally, rose to $3.86 million dollars. The likelihood of a recurring breach to a business within two years was a staggering 27.9%. More information can be found in the "2018 Cost of Data Breach" study by Ponemon:
www.ibm.com/security/data-breach .

In addition, the cost of breaches has evolved from just the cost of notification to now include ransom demands, business income loss, theft, and associated liability costs. These additional factors have also contributed to driving up the potential financial impact of a breach incident.

## Who is the insurance carrier?

The BCS Cyber and Privacy Liability Policy is underwritten by BCS Insurance Company and powered by and with the backing of certain syndicates at Lloyd's of London. BCS Insurance Company is a licensed, admitted insurance company in all states and the District of Columbia. The BCS Cyber policy is admitted in every state except VT. BCS Insurance Company provides value through a solid foundation of strong governance, national and international capabilities and product and industry expertise and israted A- (Excellent) by A.M. Best. BCS Insurance has been in business for over 60 years. It is a wholly owned subsidiary of BCS Financial Corporation which, in turn, is owned by all Blue Cross Blue Shield primary licensees.BCS Insurance Company's relationship with certain syndicates at Lloyd's of London brings additional strength, stability and industry-leading expertise to the AJG cyber insurance program. BCS was recognized by A.M. Best as the #6 Standalone Cyber Insurer in 2018, according to direct written premium, in their 2019 Best's Market Segment Report.

## What is the claims-handling process?

A 24-hour data breach hotline is available to report incidents or even suspected incidents. As soon as you suspect a data breach incident or receive notice of a claim, you should call the hotline listed in your policy. This hotline is manned by Baker Hostetler, a world-wide leading privacy law firm with experience in handling thousands of data breach events. After this initial call, Baker Hostetler will then provide on your behalf the required notice to Atheria Law PC, the designated legal firm that has been contracted to triage initial notices on behalf of the insurer. Your Gallagher broker will receive notification of the incident (or any third-party claim) as well. It is critical that you immediately report any and all incidents that you believe could give rise to a claim of any kind under this policy. You can expect Baker Hostetler to manage all breach response related activities associated with data/privacy incidents. It is also likely that interaction with representatives from Atheria Law will occur throughout the claims process for matters concerning coverage applicability, retentions, reimbursements and payment to vendors.

The information and descriptions contained in this FAQ are intended as general information and are not complete descriptions of all terms, exclusions and conditions applicable to the products and services offered by Gallagher or any insurance company represented by us. This is not a guarantee of coverage. The information contained throughout this summary is not an insurance policy or contract of insurance. The insurance coverage afforded by

Gallagher is subject to the terms and conditions of the policies as issued. This discussion is not legal advice. Gallagher does not provide legal advice and highly recommends that insureds seek legal advice of qualified legal counsel in order to become fully apprised of the legal implications related to these issues.

BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

(A stock insurance company, herein the "Company")

# Policy No. RPS-Q-50199854M/1

Cyber and Privacy Liability Insurance Policy

94.111 CT (07/19)

**NOTICE: THE POLICY CONTAINS ONE OR MORE COVERAGES. CERTAIN COVERAGES ARE LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD (OR EXTENDED REPORTING PERIOD, IF APPLICABLE). CLAIMS EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION (S). PLEASE READ THIS POLICY CAREFULLY.**

## POLICY DECLARATIONS

| | | |
|---|---|---|
| **ITEM 1.** | **NAMED INSURED** | City of Derby CT |
| | **ADDRESS** | 1 Elizabeth St , Derby, Connecticut, 06418-1801 |
| **ITEM 2.** | **POLICY PERIOD** | 12 months |
| **ITEM 3.** | **POLICY LIMITS OF LIABILITY AND COVERAGES PURCHASED** | I. Aggregate Limit of Liability: $3,000,000<br>(Aggregate for Each and Every Claim or Event including Claims Expenses)<br><br>II. Sublimit of Liability for Individual Coverage(s) Purchased: $3,000,000<br>"Nil" or "N/A" Sublimit of Liability for any coverage indicates that the coverage was not purchased |

| COVERAGE | PER CLAIM SUBLIMIT OF LIABILITY INCLUDES CLAIM EXPENSES | AGGREGATE SUBLIMIT OF LIABILITY |
|---|---|---|
| A. Privacy Liability (including Employee Privacy) | $3,000,000 | $3,000,000 |
| B. Privacy Regulatory Claims Coverage | $3,000,000 | $3,000,000 |
| C. Security Breach Response Coverage | $3,000,000 | None |
| D. Security Liability | $3,000,000 | $3,000,000 |
| E. Multimedia Liability | $3,000,000 | $3,000,000 |
| F. Cyber Extortion | $3,000,000 | None |
| G. Business Income and Digital Asset Restoration | | |
| 1.Business Income Loss | $3,000,000 | None |
| 2. Restoration Costs | $3,000,000 | None |

| | | |
|---|---|---|
| 3. Reputation Business Income Loss | $3,000,000 | None |
| 4. Systems Integrity Restoration Loss * | $250,000 | None |
| H. PCI DSS Assessment | $3,000,000 | $3,000,000 |
| I. Electronic Fraud | | |
| 1. Phishing Loss | $50,000 | None |
| 2. Services Fraud Loss | $100,000 | None |
| 3. Reward Fund Loss | $50,000 | None |
| 4. Personal Financial Loss | $250,000 | None |
| 5. Corporate Identify Theft Loss | $250,000 | None |
| 6. Telephone Hacking Loss | $100,000 | None |
| 7. Direct Financial Loss (Funds Transfer Fraud) | $100,000 | None |
| 8. Cyber Deception** | $250,000 | $250,000 |

* e.g. bricking
** e.g. social engineering

III. Supplemental Limits

| COVERAGE | SUBLIMIT OF LIABILITY |
|---|---|
| A. Court Attendance Costs | $100,000 |
| B. Bodily Injury / Property Damage Liability | $250,000 |
| C. TCPA | $100,000 |
| D. HIPAA Corrective Action Plan Costs | $50,000 |
| E. Post Breach Response | $25,000 |
| F. Independent Consultant | $25,000 |
| G. Outsourced Provider | $250,000 |
| H. Computer System | $250,000 |

**ITEM 4. RETENTION (including Claims Expenses):**

| COVERAGE | EACH CLAIM OR EVENT | AGGREGATE |
|---|---|---|
| A. Privacy Liability (including Employee Privacy) | $10,000 | $10,000 |
| B. Privacy Regulatory Claims Coverage | $10,000 | $10,000 |
| C. Security Breach Response Coverage | $10,000 | $10,000 |
| D. Security Liability | $10,000 | $10,000 |
| E. Multimedia Liability | $10,000 | $10,000 |

| | | |
|---|---|---|
| F. Cyber Extortion | $10,000 | $10,000 |
| G. Business Income and Digital Asset Restoration | $10,000 | $10,000 |
| H. PCI DSS Assessment | $10,000 | $10,000 |
| I. Electronic Fraud | | |
| 1. Phishing Loss | $10,000 | $10,000 |
| 2. Services Fraud Loss | $10,000 | $10,000 |
| 3. Reward Fund Loss | $10,000 | $10,000 |
| 4. Personal Financial Loss | $10,000 | $10,000 |
| 5. Corporate Identify Theft Loss | $10,000 | $10,000 |
| 6. Telephone Hacking Loss | $10,000 | $10,000 |
| 7. Direct Financial Loss (Funds Transfer Fraud) | $10,000 | $10,000 |
| 8. Cyber Deception | $10,000 | None |

| | | |
|---|---|---|
| **ITEM 5.** | **PREMIUM** | $18,059.00 |
| | **CYBER DECEPTION PREMIUM:** | $1,750.00 (IF ELECTED) |
| | **TRIA PREMIUM:** | $198.00 (IF ELECTED IS 1% OF THE TOTAL PREMIUM) |
| | **RPS Service Fee:** | $100.00 |
| | **TOTAL:** | $20,107.00 |
| **ITEM 6.** | **TERRITORIAL LIMITS** | Worldwide |
| **ITEM 7.** | **RETROACTIVE DATE** | Full Prior Acts |
| **ITEM 8.** | **NOTICE OF CLAIM** | Call Baker Hostetler at the 24 Hour Security Breach Hotline: 1-855-217-5204<br>Or email RPSCyberClaims@bakerlaw.com<br>Or contact:<br>BakerHostetler<br>45 Rockefeller Plaza<br>New York, NY 10111<br>Attn: RPSCyberClaims |
| **ITEM 9.** | **SERVICE OF SUIT** | Risk Situated in California:<br>Eileen Ridley<br>FLWA Service Corp.<br>c/o Foley & Lardner LLP<br>555 California Street, Suite 1700, San Francisco, CA 94104-1520<br><br>Risks Situated in All Other States: |

BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

Mendes & Mount
750 Seventh Avenue, New York, NY 10019

| | | |
|---|---|---|
| **ITEM 10.** | **CHOICE OF LAW** | Connecticut |
| **ITEM 11.** | **WAITING PERIOD:** | 12 hrs waiting period |
| **FORMS AND ENDORSEMENTS EFFECTIVE AT INCEPTION** | | 94.200 (07/19) CYBER AND PRIVACY LIABILITY POLICY FORM<br>Cyber Deception Endorsement (If elected)<br>94.102 CT (01 05) Nuclear Incident Exclusion<br>94.103 (01 15) Radioactive Contamination Exclusion<br>94.805 (06/17) Breach Response Team Endorsement<br>94.801 CT (07/19) Connecticut Amendatory Endorsement<br>94.551 (01 15) Coverage for Certified Acts of Terrorism (Included only if Terrorism coverage is elected at 1% additional premium)<br>94.554 CT (12 17) Terrorism Exclusion Endorsement |

# BCS INSURANCE COMPANY

## 2 Mid America Plaza, Suite 200
## Oakbrook Terrace, Illinois 60181

**NOTICE: THIS POLICY IS LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST YOU AND NOTIFIED TO US DURING THE POLICY PERIOD (OR EXTENDED REPORTING PERIOD, IF APPLICABLE) AS REQUIRED HEREIN, AND LOSS FROM EVENTS THAT FIRST OCCUR AFTER THE RETROACTIVE DATE AND BEFORE THE END OF THE POLICY PERIOD THAT YOU FIRST LEARN OF AND REPORT TO US DURING THE POLICY PERIOD AS REQUIRED HEREIN. CLAIMS EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION(S). TERMS THAT APPEAR IN "QUOTATIONS" HAVE SPECIAL MEANINGS. SEE THE DEFINITIONS FOR MORE INFORMATION. PLEASE READ THIS POLICY CAREFULLY.**

# CYBER AND PRIVACY LIABILITY POLICY FORM

In consideration of the payment of the premium and reliance upon the statements made by "You" in the "Application" and subject to the Limit of Liability, exclusions, conditions and other terms of this Policy, it is agreed as follows:

## I. COVERAGES

### A. PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY)

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" and reported to "Us" during the "Policy Period" or "Extended Reporting Period" arising out of a "Privacy Wrongful Act" occurring on or after the "Retroactive Date" and before the end of the "Policy Period", harming any third (3rd) party or "Employee".

### B. PRIVACY REGULATORY CLAIMS COVERAGE

"We" shall pay on "Your" behalf "Regulatory Fines", "Consumer Redress Funds", "HIPAA Corrective Action Plan Costs" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Regulatory Claim" first made against "You" and reported to "Us" during the "Policy Period" or "Extended Reporting Period" arising out of a "Privacy Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

### C. SECURITY BREACH RESPONSE COVERAGE

"We" shall pay on "Your" behalf any "Breach Response Costs" in excess of the applicable retention that are incurred in the event of a "Security Breach" with respect to "Private Information" or after a "Cyber-Extortion Threat".

"We" will not make any payment under this Coverage unless the "Security Breach" first occurs after the "Retroactive Date" and before the end of the "Policy Period" and "You" first learn of the "Security Breach" during the "Policy Period" and report the "Security Breach" to "Us" as soon as practicable within the "Policy Period".

**D. SECURITY LIABILITY**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" and reported to "Us" during the "Policy Period" or "Extended Reporting Period" arising out of a "Security Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

**E. MULTIMEDIA LIABILITY**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" and reported to "Us" during the "Policy Period" or "Extended Reporting Period" arising out of a "Multimedia Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

**F. CYBER EXTORTION**

"We" shall reimburse "You" for the "Cyber-Extortion Expenses and Cyber-Extortion Payments" that "You" actually pay in excess of the applicable retention directly resulting from a "Cyber-Extortion Threat" that "You" first receive and report to "Us" as soon as practicable during the "Policy Period".

**G. BUSINESS INCOME AND DIGITAL ASSET RESTORATION**

1. "We" shall pay "Your Organization" for the "Business Income Loss" in excess of the applicable retention that "You" sustain during a "Period of Restoration" resulting directly from a "Network Disruption" that commences during the "Policy Period", but only if the duration of such "Period of Restoration" exceeds the "Waiting Period" set forth in the Declarations, and such "Network Disruption" first occurs after the "Retroactive Date" and before the end of the "Policy Period" and "You" first learn of the "Network Disruption" during the "Policy Period" and report the "Network Disruption" to "Us" as soon as practicable within the "Policy Period".

2. "We" shall reimburse "Your Organization" for the "Restoration Costs" in excess of the applicable retention that "You" incur because of the alteration, destruction, damage or loss of "Digital Assets" that commences during the "Policy Period" resulting solely and directly from a "Security Compromise", but only if such "Security Compromise" first occurs on or after the "Retroactive Date" and before the end of the "Policy Period" and "You" first learn of the "Security Compromise" during the "Policy Period" and report the "Security Compromise" to "Us" as soon as practicable within the "Policy Period".

3. "We" shall pay "Your Organization" for the "Reputation Business Income Loss" in excess of the applicable retention that "You" sustain following a "Security Breach" or "Network Disruption", but only if such "Security Breach" or "Network Disruption" first occurs on or after the "Retroactive Date" and before the end of the "Policy Period" and "You" first learn of the "Security Breach" or "Network Disruption" during the "Policy Period" and report the "Security Breach" or "Network Disruption" to "Us" as soon as practicable within the "Policy Period".

4. "We" shall reimburse "Your Organization" for the "Systems Integrity Restoration Loss" in excess of the applicable retention caused by a "Security Compromise", but only if such "Security Compromise" first occurs on or after the "Retroactive Date" and before the end of the "Policy Period" and "You" first learn of the "Security Compromise" during the "Policy

Period” and report the “Security Compromise” to “Us” as soon as practicable within the “Policy Period”.

**H. PCI DSS ASSESSMENT**

“We” shall pay on “Your” behalf “Damages” and “Claims Expenses” that “You” become legally obligated to pay in excess of the applicable retention resulting from a “Claim” first made against “You” and reported to “Us” during the “Policy Period” or “Extended Reporting Period” arising out of a “PCI DSS Wrongful Act” occurring on or after the “Retroactive Date” and before the end of the “Policy Period”.

**I. ELECTRONIC FRAUD**

1. “We” shall reimburse “Your Organization” in excess of the applicable retention for a “Phishing Loss” caused by a "Phishing Event" first discovered by "You" and reported to "Us" during the "Policy Period".

2. “We” shall reimburse "Your Organization" in excess of the applicable retention for a “Services Fraud Loss" caused by a "Services Fraud Event" first discovered by "You" and reported to "Us" during the "Policy Period".

3. “We” shall reimburse "Your Organization" for "Reward Fund Loss" paid by "You" with "Our" prior written consent in excess of the applicable retention related to an "Event" implicating coverage under this Policy; but will not include any amount based upon information provided by "You", "Your" auditors or any individual hired or retained to investigate the illegal acts. All criminal reward funds offered pursuant to this Policy must expire no later than 6 months following the end of the "Policy Period".

4. “We” shall reimburse any senior executive officer(s) of "Your Organization" in excess of the applicable retention for "Personal Financial Loss" as a direct result of a "Security Breach" or "Security Compromise" first discovered by "You" and reported to "Us" during the "Policy Period".

5. “We” shall reimburse “Your Organization” in excess of the applicable retention for "Corporate Identity Theft Loss" incurred by "You" as a direct result of a "Security Breach" or "Security Compromise" first discovered by "You" and reported to "Us" during the "Policy Period".

6. “We” shall reimburse “Your Organization” for “Telephone Hacking Loss” in excess of the applicable retention arising from a “Telephone Hacking Event” first discovered by “You” during the “Policy Period” as a direct result of “Your” “Telecommunications Services” being subject to a “Telephone Hacking Event” arising from unauthorized calls or unauthorized use of “Your” bandwidth, but only if "You" first learn of the "Telephone Hacking Event" during the "Policy Period" and report the "Telephone Hacking Event" to "Us" as soon as practicable within the "Policy Period."

7. “We” shall reimburse “Your Organization” for “Direct Financial Loss” as a direct result of "Funds Transfer Fraud" committed by a third party and first discovered by “You” and reported to "Us" during the “Policy Period”.

8. In consideration of the required additional premium for optional Cyber Deception coverage, “We” shall reimburse “Your Organization” per the terms and conditions of the Cyber Deception Endorsement attached to this policy.

**II. DEFENSE, SETTLEMENT, AND INVESTIGATION OF CLAIMS**

A. “We” shall have the right and duty to defend, subject to the “Policy Aggregate Limit” and applicable “Sublimits of Liability”, exclusions and other terms and conditions of this Policy, any “Claim” against “You” seeking “Damages” which are potentially payable under the terms of this Policy, even if any of the allegations of the “Claim” are groundless, false, or fraudulent.

“You” and “We” shall mutually agree on counsel to defend “Claims”. “You” shall not formally appoint defense counsel without “Our” consent, which shall not be unreasonably withheld. However, in the absence of such agreement, “Our” choice of counsel decision shall control. “We” agree that “You” may settle any “Claim” where the “Damages” and “Claims Expenses” do not exceed fifty percent (50%) of the applicable retention, provided that the entire “Claim” is resolved and “You” receive a full release from all claimants.

“We” shall have the right to make any investigation We” deem necessary, including without limitation, any investigation with respect to the “Application” and statements made in the “Application” and with respect to potential coverage.

The “Policy Aggregate Limit” and “Sublimits of Liability” available to pay “Damages”, “Claims Expenses” and “Loss” shall be reduced and may be completely exhausted by payment of such. “Damages”, “Claims Expenses” and “Loss” and shall be applied against the applicable retention “You” pay.

B. If “You” refuse to consent to a settlement or compromise “We” recommend, which settlement or compromise is acceptable to the claimant, and “You” elect to contest the “Claim”, then:

1. Subject to the applicable Limits of Liability, our liability for any “Damages” and “Claims Expenses” shall not exceed:

   a. the amount for which the “Claim” could have been settled, plus the “Claims Expenses” incurred up to the date of such refusal; and

   b. eighty percent (80%) of the “Damages” and “Claims Expenses” in excess of the amount in a. above incurred for such “Claim”; provided that “You” bear the remaining twenty percent (20%) of the “Damages” and “Claims Expenses” in excess of the amount in a. above as uninsured and at “Your” own risk; and

2. “We” shall have the right to withdraw from the further defense of such “Claim” by tendering control of the defense to “You”.

This clause shall not apply to any settlement where the total of the proposed settlement and incurred “Claims Expenses” do not exceed all applicable retentions.

C. “We” shall not be obligated to pay any “Damages”, “Claims Expenses” or “Loss” or to undertake or continue any defense of any “Claim”, after the “Policy Aggregate Limit” or applicable “Sublimit(s) of Liability” have been exhausted by payment of “Damages”, “Claims Expenses” and/or “Loss” or after deposit of the “Policy Aggregate Limit” or applicable “Sublimit(s) of Liability” in a court of competent jurisdiction, and that upon such payment or deposit, “We” shall have the right to withdraw from the further defense thereof by tendering control of said defense to “You”.

## III. TERRITORY

This insurance applies to “Events” occurring, “Claims” made and “Wrongful Acts”, acts, errors or omissions committed or alleged to have been committed anywhere in the world.

## IV. EXCLUSIONS

The coverage under this Policy shall not apply to any “Damages”, Claims Expenses”, “Loss” or other amounts, arising out of or resulting directly, from:

A. “Bodily Injury” or “Property Damage”; except:

   1. with respect to a "Claim" under Coverages A. Privacy Liability and D. Security Liability only, this exclusion will not apply to any otherwise covered "Claim" for emotional distress mental injury, mental tension or mental anguish, pain and suffering, humiliation or shock; and

   2. Except for a "Claim" described in Section IV.A.1., with respect to a "Claim" under Coverages A. Privacy Liability and D. Security Liability only, this exclusion will not apply to any otherwise covered claim for "Bodily Injury" or "Property Damage" but the most "We" will pay for such "Bodily Injury" or "Property Damage" is the sublimit of liability stated in ITEM 3.III.B. of the Declarations. Such sublimit is part of the Limit of Liability and not in addition.

   3. This exclusion will also not apply to a “Systems Integrity Restoration Loss” covered under Coverages G.4.

B. “Your” employment practices or any alleged or actual discrimination against any person or entity on any basis, including without limitation, race, creed, color, religion, ethnic background, national origin, age, handicap, disability, sex, sexual orientation, or pregnancy; provided, however, this exclusion shall not apply to any “Claim” alleging a “Privacy Wrongful Act” or “Security Wrongful Act” in connection with an “Employee’s” or prospective employee’s employment;

C. The failure, malfunction or inadequacy of any satellite; any electrical or mechanical failure and/or interruption, including but not limited to electrical disturbance, spike, brownout or blackout; or any outage to gas, water, telephone, cable, telecommunications or other infrastructure, unless such infrastructure is under “Your” operational control; provided, however this exclusion shall not apply to any “Privacy Wrongful Act” that is caused by such electrical or mechanical failure or that is caused by such failure of telephone lines, data transmission lines or other infrastructure comprising or supporting the “Internet”;

D. Fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, an act of God or any other physical event, however caused;

E. Breach of any express, implied, actual or constructive contract, agreement, warranty, guarantee or promise, provided, however, this exclusion shall not apply to:

   1. any liability or obligation “You” would have in the absence of such contract or agreement;

   2. any breach of “Your” privacy statement; or

   3. any indemnity by “You” in a written contract or agreement with “Your” client regarding any “Privacy Wrongful Act” or “Security Wrongful Act” by “You” in failing to preserve the confidentiality or privacy of “Private Information”;

   4. any "Merchant Service" Agreement that “You” may enter into as part of "Your" business activities.

F. Any of the following:

   1. Any presence of pollutants or contamination of any kind;

   2. Any actual, alleged or threatened discharge, dispersal, release, or escape of pollutants or contamination of any kind;

3. Any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize pollutants or in any way respond to or assess the effects of pollutants or contamination of any kind;

4. Manufacturing, mining, use, sale, installation, removal, distribution of or exposure to asbestos, materials, or products containing asbestos, asbestos fibers or dust;

5. Ionizing radiation or contamination by radioactivity from any nuclear fuel or any nuclear waste from the combustion of nuclear fuel;

6. Actual, potential or alleged presence of mold, mildew or fungi of any kind;

7. The radioactive, toxic, or explosive or other hazardous properties of any explosive nuclear assembly or nuclear component thereof; or

8. 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;

G. Any of the following:

1. the purchase, sale, offer of or solicitation of an offer to purchase or sell securities, or alleged or actual violation of any securities law, including but not limited to the provisions of the Securities Act of 1933 or the Securities Exchange Act of 1934, as amended, the Sarbanes-Oxley Act of 2002, or any regulation promulgated under the foregoing statutes, or any federal, state, local or foreign laws similar to the foregoing statutes (including “Blue Sky” laws), whether such law is statutory, regulatory or common law. However, this exclusion G.1. does not apply to any “Claim” alleging or arising out of a violation of Regulation S-P (17 C.F.R. §248) or any failure to disclose a “Security Breach” or violation of any “Privacy Regulation”;

2. alleged or actual 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 federal, state, local or foreign law similar to the foregoing statute, whether such law is statutory, regulatory or common law, unless the "Claim" results from "Your" alleged introduction of malicious code that results in the theft, loss or unauthorized disclosure of the claimant's "Private Information";

3. alleged or actual violation of the responsibilities, obligations or duties imposed upon fiduciaries by the Employee Retirement Income Security Act of 1974, as amended unless the "Claim" results from "Your" alleged introduction of malicious code that results in the theft, loss or unauthorized disclosure of the claimant's "Private Information"; or

4. alleged or actual anti-trust violations, restraint of trade or unfair competition, including without limitation, violations of the Sherman Act, the Clayton Act or the Robinson-Patman Act, or any other federal, state, local, or foreign laws regulating the same or similar conduct; provided, however, this exclusion G.4 shall not apply to a “Claim” for a “Multimedia Wrongful Act” or a “Regulatory Claim”;

H. Any “Act Of Terrorism”; strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular uprising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against

these actions; including all amounts, “Damages”, “Claims Expenses” or “Loss” 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 the above; provided, however, if “We” allege that by reason of this exclusion any “Damages”, “Claims Expenses” or “Loss” are not covered by this Policy, the burden of proving the contrary shall be upon “You”. However, this exclusion does not apply to acts perpetrated electronically;

I. Any of the following:

1. any circumstance or “Event” occurring, or “Wrongful Act”, act, error, or omission committed, prior to the inception date of this Policy or, if this is a renewal, prior to the first date of this type of insurance granted by “Us” or any other insurer, that a member of the “Control Group” knew, or could have reasonably foreseen that such circumstance, “Event”, “Wrongful Act”, act, error, or omission would be the basis of a “Claim” or lead to an “Event”;

2. any “Claim”, “Event” or circumstance of which notice was provided to “Us” or another insurer prior to the “Policy Period” that was, could reasonably be expected to be, or lead to, the type of “Claim” or “Event” potentially covered by this Policy; or

3. any circumstance occurring or “Event” commencing, or “Wrongful Act”, act, error, or omission committed prior to the “Retroactive Date”;

J. Any criminal conduct, dishonest act, intentional violation of the law, unfair or deceptive business practice, fraudulent or malicious act, or error or omission committed by “You” with actual criminal, dishonest, fraudulent or malicious purpose or intent; provided, however, this exclusion shall not apply to:

1. “Claims Expenses” incurred in defending any such “Claim” until there is a final adjudication, judgment, binding arbitration decision or conviction against “You” in such “Claim” or an admission by “You” establishing such conduct, or a plea of nolo contendere or no contest by “You” regarding such conduct, in which event “You” shall reimburse “Us” for all “Claims Expenses” that “We” have paid and “We” shall have no further liability for “Claims Expenses” from such “Claim”; and

2. any of “You” who did not personally commit, personally participate in committing or personally acquiesce in such conduct, except that this exclusion shall apply with respect to “Your Organization” if an admission, final adjudication, or finding in a proceeding separate or collateral to the “Claim” establishes that a current member of the “Control Group” in fact engaged in such conduct;

K. Any “Claim” made by or on behalf of:

1. any person or entity within the definition of “You” against any other Insured person or entity within the definition of “You”; provided, however, this exclusion shall not apply to an otherwise potentially covered “Claim” under Coverage A made by a current or former “Employee” of “Your Organization”; or

2. any entity which:

a. is operated, managed, or controlled by “You” or in which “You” have an ownership interest in excess of twenty five percent (25%) or in which “You” are an officer or director; or

b. operates, controls, or manages “Your Organization”, or has an ownership interest of more than twenty five percent (25%) in “Your Organization”;

L. “Your” activities as a trustee, partner, officer, director, or “Employee” of any employee trust, charitable organization, corporation, company or business other than “Your Organization”;

M. Any alleged or actual:

1. infringement or violation of patent rights; or

2. misappropriation, theft, copying, display or publication of any trade secret;

Unless such event occurs as a result of a “Security Compromise”.

N. Any trading losses or trading liabilities; the monetary value of any electronic fund transfers or transactions by or on behalf of “You” which is lost, diminished, or damaged during transfer from, into or between accounts; or the face value of coupons, price discounts, prizes, awards, or any other valuable consideration given in excess of the total contracted or expected amount; provided, however, this exclusion will not apply to any “Breach Response Costs” incurred due to a “Security Breach”.

O. Any actual or alleged violation of the Telephone Consumer Protection Act (the "TCPA"); however, this exclusion will not apply to a "Claim" against "You" for violation of the TCPA otherwise covered under Insuring Agreements A or B; however, the most "We" will pay for "Claims Expenses" or "Damages" under this exception to this exclusion is the sublimit of liability stated in ITEM 3.III.C. of the Declarations. Such sublimit is part of the Limit of Liability and not in addition.

With respect to Coverage G only, this Policy does not apply to any “Damages”, “Claims Expenses”, "Loss" or other amounts arising out of, or resulting, directly or indirectly from:

P. Any failure of:

1. telephone lines;

2. data transmission lines or wireless communications connection; or

3. other telecommunications equipment, facilities or electronic infrastructure, including equipment, facilities or infrastructure that supports the operation of computer networks, including the “Internet”, which are used to transmit or receive voice or data communications and which are not under “Your” direct operational control or, if applicable, not under the direct operational control of “Your” “Service Provider”;

Q. Any seizure, confiscation, nationalization, or destruction of, or damage to or loss of use of any “Digital Asset” or “Your” “Computer Systems” by order of any governmental authority;

R. Ordinary wear and tear or gradual deterioration of “Digital Assets” or “Computer Systems” on which “Digital Assets” are processed or stored, whether owned by “You” or others; or

S. The physical loss of, damage to or destruction of tangible property, including the loss of use thereof; however, “tangible property” does not include “Digital Assets”, but does include all computer hardware unless otherwise covered as “Systems Integrity Restoration Loss”.

**NOTE: Exclusions P through S apply to Coverage G only.**

## V. DEFINITIONS

"Acquiring Bank" means a bank or financial institution that accepts credit and/or debit payments (including credit cards, debit cards, stored value cards and pre-paid cards) for products or services on behalf of a merchant, including processing and crediting those payments to a merchant.

"Act Of Terrorism" means:

1. any act certified an "Act Of Terrorism" pursuant to the federal Terrorism Risk Insurance Act of 2002 or otherwise declared an "Act Of Terrorism" by any government;

2. any act committed by any person or group of persons designated by any government as a terrorist or terrorist group or any act committed by any person or group of persons acting on behalf of or in connection with any organization designated by any government as a terrorist organization; or

3. the use of force or violence and/or the threat thereof by any person or group of persons, whether acting alone or on behalf of or in connection with any organization or government, committed for political, religious, ideological, or similar purposes, including the intention to influence any government and/or put the public, or any section of the public, in fear.

"Application" means all applications, including any attachments thereto, and all other information and materials submitted by "You" or on "Your" behalf to "Us" in connection with the underwriting of this Policy.

"Bodily Injury" means injury to the body, sickness, or disease sustained by any person, and where resulting from such injuries, mental anguish, mental injury, shock, humiliation, emotional distress, loss of consortium, or death.

"Breach Response Costs" means the following fees, costs, charges or expenses, if reasonable and necessary, that our "Breach Response Team" incurs in responding to a "Security Breach" or a "Cyber-Extortion Threat", or the following costs described in subparagraphs 1 through 9 and incurred by a non-panel vendor with "Our" prior written agreement because of a "Security Breach" experienced by "You", so long as such costs are incurred during the period of twelve (12) months after "You" first learn of such "Security Breach":

1. forensic professional fees and expenses to determine the cause and extent of such "Security Breach" and terminate the "Security Breach";

2. "Breach Response Counsel" fees and expenses to: determine whether "You" or a third party are obligated under applicable "Privacy Regulations" to notify applicable regulatory agencies or individuals affected or reasonably believed to be affected by such "Security Breach"; effect compliance with any applicable "Privacy Regulations"; draft the text of privacy notifications to individuals affected or reasonably believed to be affected by such "Security Breach"; notify law enforcement; and, coordinate the investigation of such "Security Breach";

3. costs to notify individuals affected or reasonably believed to be affected by such "Security Breach", including printing costs, publishing costs, postage expenses, call center costs or costs of notification via phone or e-mail, including "voluntary notification" where "You" or a third party have no legal obligation to provide notification, but wish to do so to protect "Your" or a third party's brand and reputation, and the costs to notify regulators if required to do so;

4. "Credit Monitoring Expenses";

5. identity theft restoration costs;

6. public relations expenses;

7. the cost of a PCI Forensic Investigator (PFI) fees/expenses and a second forensic investigator to shadow the PFI following a “Security Breach"; and

8. reasonable and necessary fees for a mandatory audit by a Qualified Security Assessor (QSA) to show “You” are PCI Data Security Standards compliant following a “Security Breach".

9. the reasonable and necessary costs, not to exceed the sublimit of liability stated in ITEM 3.III.E. of the Declarations and implemented by the members of the "Breach Response Team" identified as Post Breach Response service providers, of the following: (1) the revision of an incident response plan; (2) the completion of a network security audit; (3) an information security risk assessment; or (4) the implementation of a security awareness training program;

“Breach Response Costs” do not include “Your” overhead expenses or any salaries, wages, fees, or benefits of “Your” “Employees”.

“Breach Response Counsel” means counsel approved in the Breach Response Team Endorsement and counsel as appointed by “Us”.

“Breach Response Team” means the vendors approved in the Breach Response Team Endorsement and vendors approved by “Us”.

“Business Income Loss” means:

1. “Earnings Loss”;

2. “Expenses Loss”; and/or

3. The reasonable and necessary costs "You" incur to retain an Independent Consultant to determine the amount of "Your" "Business Income Loss", not to exceed the sublimit stated in ITEM 3.III.F. of the Declarations. This sublimit of liability is part of, and not in addition to, the sublimit of liability stated in ITEM 3.II.G.1. of the Declarations.

The most “We” will pay for “Business Income Loss” that “You” sustain resulting directly from a “Network Disruption” involving an “Outsourced Provider” “Computer System” (as defined in part 2. of the Definition of "Network Disruption") is the sublimit stated in ITEM 3.III.G. of the Declarations. This sublimit of liability is part of, and not in addition to, the sublimit of liability stated in ITEM 3.II.G.1. of the Declarations.

“Business Income Loss” does not include:

1) any contractual penalties;

2) any costs or expenses incurred to update, upgrade, replace, restore or otherwise improve any “Computer System” to a level beyond that which existed prior to a “Network Disruption”;

3.) any costs or expenses incurred to identify, remove or remediate computer program errors or vulnerabilities, or costs to update, upgrade, replace, restore, maintain or otherwise improve any “Computer System”;

4) any legal costs or expenses or other amounts arising out of liability to any third (3rd) party;

5) any amounts incurred as a result of unfavorable business conditions; or

6) any other consequential amounts, loss or damage.

“Claim” means:

1. A written demand received by “You” for money or services, including the service of a civil suit or institution of arbitration proceedings;

2. Initiation of a civil suit against “You” seeking injunctive relief;

3. A written notice of an alleged "Privacy Wrongful Act" or "Security Wrongful Act" from a third party.

4. Solely with respect to Coverage B., a “Regulatory Claim” made against “You”; or

5. Solely with respect to Coverage H., written notice to "You" of a “PCI DSS Assessment”.

Multiple “Claims” arising from the same or a series of related or repeated “Wrongful Acts”, acts, errors, or omissions or from any continuing “Wrongful Acts”, acts, errors or omissions shall be considered a single “Claim” for the purposes of this Policy, irrespective of the number of claimants or “You” involved therein. All such related “Claims” shall be deemed to have been first made at the time the earliest such “Claim” was made or deemed made under Section IX.A.

“Claims Expenses” means:

1. reasonable and necessary fees charged in the defense or settlement of a “Claim” by an attorney whom “We” designate or whom “You” designate with “Our” prior written consent, such consent not to be unreasonably withheld; and

2. all other legal costs and expenses resulting from the investigation, adjustment, defense and appeal of a “Claim”, if incurred by “Us” or by “You” with “Our” prior written consent; however, “Claims Expenses” do not include “Your” overhead expenses or any salaries, wages, fees, or benefits of “Your” “Employees” for any time spent in cooperating in the defense or investigation of any “Claim” or circumstance that might lead to a “Claim”.

3. Notwithstanding the foregoing, "Claims Expenses" includes Court Attendance Costs, defined as reasonable sums necessarily incurred by "You" with "Our" prior written agreement, not to exceed the sublimit of liability stated in ITEM 3.III.A. of the Declarations, to attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any "Claim" for which "You" are entitled to a defense under this Policy.

“Computer System” means electronic, wireless, web or similar systems (including all hardware and software) used to process data or information in an analog, digital, electronic or wireless format, including computer programs, electronic data, operating systems, and components thereof, including but not limited to laptops, personal digital assistants, cellular phones, media storage and peripheral devices, including the internet of things (IoT) devices, media libraries, associated input and output devices, networking identity equipment, and electronic backup equipment. With respect to Coverage G only, “Computer System” means a “Computer System” over which “You” have direct operational control or that is under the direct operational control of a “Service Provider” used to process, maintain or store “Your” “Digital Assets”.

“Consumer Redress Funds” means any sums of money “You” are legally required to deposit in a fund for the payment of consumers due to a settlement of, or an adverse judgment in, a “Regulatory Claim”.

“Control Group” means the board members, executive officers, Chief Technology Officer, Chief Information Officer, Risk Manager and General Counsel or their functional equivalents of “Your Organization”. This does not include any administrative staff who work in the offices of these named positions.

"Corporate Identity Theft Loss" means monetary or other financial asset loss as a result of the fraudulent use of "Your" electronic identity, including the establishment of credit in "Your" name, the electronic signing of any contract, or the creation of any website designed to impersonate "You". The most “We” will pay for any “Corporate Identity Theft Loss” is the sublimit of liability stated in ITEM 3.II.I.5. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

“Credit Monitoring Expenses” means the reasonable and necessary expense of providing free credit report services, identity theft protection services, credit monitoring services, credit freezes, healthcare fraud monitoring services, fraud alerts or call center services for customers, third parties and employees affected or reasonably believed to be affected by a “Security Breach”. However, “We” shall not be obligated to pay for more than twelve (12) months from the date of enrollment in such services, unless there is a statute, rule, regulation, court ruling or requirement by a regulator requiring otherwise, or in the opinion of “Breach Response Counsel”, offering more than twelve (12) months will justifiably reduce “Your” potential liability, “Damages” or “Loss”.

“Cyber-Extortion Expenses” means the reasonable and necessary expenses “You” incur with “Our” approval in evaluating and responding to a “Cyber-Extortion Threat”. However, “Cyber-Extortion Expenses” do not include “Your” overhead expenses or any salaries, wages, fees, or benefits of “Your” “Employees”.

“Cyber-Extortion Payment” means any sum paid to or at the direction of any third (3rd) party, including sums paid via bitcoin or other crypto currencies, that “You” reasonably believe to be responsible for a “Cyber-Extortion Threat”; provided that:

1. “You” obtain “Our” written consent prior to making such “Cyber-Extortion Payment”;

2. “You” make such “Cyber-Extortion Payment” to terminate the “Cyber-Extortion Threat”; and

3. the “Cyber-Extortion Payment” does not exceed the amounts “We” reasonably believe would have been incurred had such “Cyber-Extortion Payment” not been made.

“Cyber-Extortion Threat” means a credible threat or connected series of threats made, or actions taken, by someone other than a member of the “Control Group”:

1. to introduce “Malicious Code” into “Your” “Computer System”;

2. to interrupt “Your” “Computer System” or interrupt access to “Your” “Computer System”, such as through a “Denial of Service Attack”;

3. to corrupt, damage or destroy “Your” “Computer System”; or

4. to disseminate, divulge, or improperly utilize any “Private Information” on “Your” “Computer Systems” taken as a result of a “Network Disruption”.

“Damages” means:

1. Solely with respect to Coverages A, D, or E, a monetary judgment, award or settlement, including:

a. Pre-judgment interest;

b. Post-judgment interest that accrues after entry of the judgment or award and before “We” have paid, offered to pay or deposited in court that part of the judgment or award within the applicable Limits of Liability;

c. subject to this Policy’s terms, conditions, and exclusions, punitive or exemplary “Damages” (where insurable by the applicable law that most favors coverage for such “Damages”);

d. liquidated damages, contractual service credits or contractual penalties but not exceeding those “You” would have been liable for in the absence of such contract;

2. Solely with respect to Coverage B, “Regulatory Fines” and “Consumer Redress Funds”; and

3. Solely with respect to Coverage H, a "PCI DSS Assessment" or a settlement of a "PCI DSS Assessment".

“Damages” shall not include or mean:

1) “Your” future profits, restitution, or disgorgement of profits; or “Your” cost to comply with any order granting injunctive or non-monetary relief, including specific performance, or any agreement to provide such relief;

2) “Your” return or offset of fees, charges, royalties, or commissions for goods or services already provided or contracted to be provided;

3) fines or penalties of any nature, except those that are part of “Regulatory Fines” and “Consumer Redress Funds” as identified above, or sought in a “PCI DSS Assessment”;

4) any amount “You” are not financially or legally obligated to pay;

5) any donations or contributions to any charitable organization;

6) charge backs, interchange fees, discount fees or prospective services fees sought, awarded or agreed to as part of a settlement in a “PCI DSS Assessment”; or

7) matters that may be deemed uninsurable under law. “We” shall apply the most favorable state law to “You” in determining insurability.

“Denial of Service Attack” means unauthorized attacks or deliberate overloading of bandwidth connections and/or web servers by means of the sending of substantial quantities of repeat or irrelevant communication or data with the intent of blocking access to “Your” “Computer System” through the “Internet” by third (3rd) parties.

“Digital Assets” means any electronic data, including personally identifiable, non-public information, or computer software over which “You” have direct control or for which such control has been contractually assigned by “Your Organization” to a “Service Provider”. “Digital Assets” do not include computer hardware of any kind.

"Direct Financial Loss" means "Your” monetary or other financial asset loss as a result of a “Funds Transfer Fraud” under Coverage I. The most “We” will pay for any “Direct Financial Loss” arising from

a “Funds Transfer Fraud” is the sublimit of liability stated in ITEM 3.II.I.7. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

“Earnings Loss” means the difference between the revenue that “Your Organization” would have earned, based on reasonable projections and the variable costs that would have been incurred, but which “Your Organization” would have saved as a result of not earning that revenue.

“Employee” means any individual in “Your Organization’s” service, including any part-time, seasonal, and temporary employee, who is compensated by salary, wages, fees or commissions, or unpaid intern or volunteer over whom “You” have the right to direct and control, but excluding any partner or director of “Your Organization”.

“Event” means a:

1. “Security Breach”;

2. “Cyber-Extortion Threat”;

3. “Security Compromise”;

4. “Network Disruption;

5. "Phishing Event";

6. "Services Fraud Event";

7. “Telephone Hacking Event”; or

8. "Funds Transfer Fraud".

Multiple “Events” arising from the same or a series of related or repeated “Events”, acts, errors, or omissions, or from any continuing “Events”, acts, errors, or omissions shall be considered a single “Event” for the purposes of this Policy. All such related “Events” shall be deemed to have first occurred at the time the earliest such “Event” first occurred or commenced.

“Expenses Loss” means the additional expenses “Your Organization” incurred to minimize the suspension of business and to continue operations that are over and above the expenses that “Your Organization” reasonably and necessarily would have incurred to conduct “Your” business had no “Network Disruption” occurred. These additional expenses do not include any " “Restoration Costs” or any actual, reasonable and necessary expenses “You” incur in response to a “Network Disruption” in order to prevent, minimize or mitigate any further damage to “Your” “Digital Assets”, or preserve critical evidence of any wrongdoing.

“Extended Reporting Period” means the period of time after the end of the “Policy Period” for reporting “Claims” as provided in Section VIII. of this Policy.

"Funds Transfer Fraud" means any of the following acts, carried out by means other than through the intentional misleading of a person by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and relied upon by a person believing it to be genuine:

1. any unauthorized electronic funds transfer;

2. theft of “Your” money or other financial assets from "Your" bank by electronic means;

3. theft of money or other financial assets from “Your” corporate credit cards by electronic means; or

4. any fraudulent manipulation of electronic documentation while stored on “Your” ”Computer System”.

"HIPAA Corrective Action Plan Costs" means reasonable and necessary costs "You" incur with "Our" prior written approval, not to exceed the sublimit of liability stated in ITEM 3.III.D. of the Declarations, to meet any of the requirements specified within a HIPAA corrective action plan as the direct result of a “Regulatory Claim” otherwise covered by this "Policy".

“Intranet” means a private computer network inside a company or organization that uses the same kinds of software found on the “Internet”, but only for internal use.

“Internet” means the worldwide public network of computer networks which enables the transmission of electronic data between different users, commonly referred to as the “Internet”, including a private communications network existing within a shared or public network platform.

“Loss” means a:

1. “Business Income Loss”;

2. “Breach Response Costs”;

3. “Reputation Business Income Loss”;

4. “Restoration Costs”;

5. "System Integrity Restoration Loss";

6. “Cyber-Extortion Payments” and “Cyber-Extortion Expenses”;

7. "Phishing Loss";

8. "Services Fraud Loss"';

9. "Reward Fund Loss";

10. "Personal Financial Loss";

11. "Corporate Identity Theft Loss";

12. "Telephone Hacking Loss"; or

13. "Direct Financial Loss".

“Malicious Code” means any unauthorized and corrupting or harmful computer code, including but not limited to computer viruses, spyware, Trojan horses, worms, logic bombs, and mutations of any of the proceeding.

“Media Content” means data, digital code, images, graphics, sounds, text or any other similar material regardless of the method or medium of communication of such content or the purpose of the communication.

"Merchant Services Agreement" means any written agreement between “You” and a card association (including MasterCard, VISA, Discover, American Express or JCB), which allows “You” to accept payment by credit, debit or prepaid card.

“Multimedia Wrongful Act” means any of the following acts committed in the ordinary course of “Your Organization’s” business in gathering, communicating, reproducing, publishing, disseminating, displaying, releasing, transmitting or disclosing “Media Content” via any “Computer System” that “You” own or operate or is operated on “Your” behalf by a third (3rd) party, including any web-based social media authorized or operated by “Your Organization” or any “Internet” or “Intranet” website, or via any non-electronic media:

1. defamation, libel, slander, product disparagement, 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;

2. invasion of or interference with the right to privacy or publicity;

3. false arrest, detention or imprisonment or malicious prosecution;

4. infringement of any right to private occupancy, including trespass, trespass as a result of cookie use, wrongful entry, eviction or eavesdropping;

5. infringement of copyright, domain name, trade dress, title or slogan, or the dilution or infringement of trademark, service mark, service name or trade name;

6. plagiarism, piracy or misappropriation of ideas;

7. improper deep linking; or

8. other conduct causing liability regarding any” Media Content” for which “You” are responsible;

provided always that any “Multimedia Wrongful Act” was committed or alleged to have been committed by “You”, or any person for whom or entity for which “You” are legally responsible, including an independent contractor or outsourcing organization.

“Network Disruption” means any of the following incidents:

1. an unplanned failure, interruption or degradation of the operation of “Your” “Computer System” or the denial, restriction or hindrance of access to or use of “Your” “Computer System" or “Your” “Digital Assets” by any party who is otherwise authorized to have access; and

2. with respect to Coverage G.1 only, "Network Disruption" also means an unplanned failure, interruption or degradation of the operation of an “Outsourced Provider” “Computer System”; or the denial, restriction or hindrance of access to or use of an “Outsourced Provider” “Computer System” by any party who is otherwise authorized to have access.

Solely with respect to Coverage G.1.:

3. the voluntary and intentional shutdown of "Computer Systems" by "You" but only to the extent necessary to mitigate the "Loss" resulting from a situation described in Section V. Definitions, “Security Compromise” 1. or 2.; or

4. the intentional shutdown of "Computer Systems" by "You" as expressly required by any federal, state, local or foreign governmental entity in such entity’s regulatory or official

capacity resulting from a situation described in Section V. Definitions, “Security Compromise” 1. or 2.

More than one such incident that results from the same or related underlying facts, circumstances, situations, transactions or “Security Compromises” shall be considered a single “Network Disruption” which first occurs on the date of the earliest of such events.

“Outsourced Provider” means any provider, other than a “Service Provider”, that “You” do not own, operate, or control, that performs services, other than IT services, for “You” pursuant to a written contract. An “Outsourced Provider” does not include any provider of “Telecommunications Services” including “Internet” access to “You”.

“PCI DSS Assessment(s)” means amounts legally owed by "You" to "Your" acquiring bank or a card association (MasterCard, VISA, Discover, American Express or JCB) for monetary fines, penalties, reimbursements, fraud recoveries or assessments, due to "Your" actual or alleged non-compliance with PCI Data Security Standards further to the terms of a "Merchant Services Agreement".

“PCI Data Security Standards” (known as PCI DSS) means the published data security standard in effect now or as hereafter amended that all merchants and processors must follow when storing, processing and transmitting cardholder data.

“PCI DSS Wrongful Act” means “Your” actual or alleged non-compliance with “PCI Data Security Standards”.

“Period of Restoration” means the time period from the commencement of a "Network Disruption" to the earlier of the following dates:

1. the date "Your" "Computer System", "Outsourced Provider" "Computer System" or "Your" "Digital Assets" are restored to the condition and functionality that existed immediately prior to the "Network Disruption;" or

2. the date "Your" "Computer System", "Outsourced Provider" "Computer System" or "Your" "Digital Assets" with reasonable diligence, could have been restored to the condition and functionality that existed immediately prior to the "Network Disruption."

"Personal Financial Loss" means monetary or other financial asset loss as a result of:

1. theft of money or other financial assets from a personal bank account of the senior executive officer; or

2. identity theft of the senior executive officer.

The most “We” will pay for any “Personal Financial Loss” is the sublimit of liability stated in ITEM 3.II.I.4. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

“Phishing Event” means the impersonation of “You” by a third party via email or other electronic communications.

“Phishing Loss” means an unpaid account receivable held by "You", or an inability to collect funds owed to "You" by a third party, caused by a "Phishing Event". The most “We” will pay for any “Phishing Loss” is the sublimit of liability stated in ITEM 3.II.I.1. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

“Policy Period” means the period of time beginning on the date stated in ITEM 2 of the Declarations and ending on the earlier of the expiration date stated in ITEM 2 of the Declarations or the effective date of the cancellation of the Policy. If "You" become an insured under the Policy, the "Policy Period" begins on the date "You" become an insured.

“Privacy Breach” means a common law breach of confidence, infringement, or violation of any rights to privacy, including but not limited to breach of “Your” privacy statement, breach of a person’s right of publicity, wrongful collection, false light, intrusion upon a person’s seclusion, public disclosure of “Private Information”, or misappropriation of a person’s picture or name for commercial gain.

“Privacy Regulations” means any federal, state, local or foreign statute or regulation requiring “You” to limit or control the collection, use of, or access to, “Private Information” in “Your” possession or under “Your” control, or obligating “You” to inform customers of the “Unauthorized Access” or disclosure of such personally identifiable, non-public information, including but not limited to the following statutes and regulations:

1. the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), including Title II requiring protection of confidentiality and security of electronic protected health information, and as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), any rules and regulations promulgated thereunder as they currently exist and as amended, and any related state medical privacy laws as they currently exist and as amended;

2. the Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act of 1999, including sections concerning security protection and standards for customer records maintained by financial services companies, and the rules and regulations promulgated thereunder as they currently exist and as amended;

3. Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. 45(a), but solely with respect to alleged unfair or deceptive acts or practices in or affecting commerce;

4. federal, state or local privacy protection regulations or laws, such as the California Database Protection Act of 2003 (previously called SB 1386), as they currently exist now or may be amended, associated with the control and use of, or limiting “Unauthorized Access” to, personal information, including but not limited to requirements to post privacy policies, adopt specific privacy controls, or inform customers of breaches of security that has or may impact their personal information;

5. federal, state or local data breach regulations or laws, as they currently exist now or in the future, imposing liability for failure to take reasonable care to guard against “Unauthorized Access” to credit or debit account information that is in “Your” possession or under “Your” control;

6. identity theft red flags under the Fair and Accurate Credit Transactions Act of 2003;

7. federal and state consumer credit reporting laws, such as the Federal Fair Credit Reporting Act (FCRA) and the California Consumer Credit Reporting Agencies Act (CCCRAA);

8. the Children’s Online Privacy Protection Act of 1998; and

9. privacy protection regulations or laws adopted by countries outside of the United States, such as the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), as they currently exist now or may be amended, associated with the collection, control and use of, or limiting “Unauthorized Access” to, personal information.

"Privacy Wrongful Act" means any "Privacy Breach" or breach of "Privacy Regulations" actually or allegedly committed by "You" or by any person or entity for which "You" are legally responsible, including an independent contractor or outsourcing organization.

"Private Information" means any:

1. proprietary or confidential information owned by a third party or "You";

2. information that can be used to determine, distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual;

3. information concerning an individual that would be considered personal data or sensitive personal data within the meaning of the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) and any amendments thereto; or

4. "Your" corporate confidential information that relates to "Your" organization's business operations, activities and procedures.

"Property Damage" means physical injury to or destruction of any tangible property, including the loss of use thereof. Electronic data is not considered tangible property.

"QSA Audit" is an audit required by PCI Security Standards Council and conducted by a Qualified Security Assessor employed by a qualified QSA auditor.

"Regulatory Claim" means:

1. any request for information, civil investigative demand or formal investigation of "You" by an administrative or regulatory agency or similar governmental body concerning a "Privacy Breach" or possible breach of "Privacy Regulations"; or

2. any administrative or civil proceeding against "You" by an administrative or regulatory agency, supervisory authority, authorized data protection authority or similar governmental body for a breach of "Privacy Regulations".

"Regulatory Fines" means fines, penalties, or sanctions awarded for a violation of any "Privacy Regulation".

"Reputation Business Income Loss" means:

1. "Earnings Loss" and/or

2. "Expenses Loss";

solely due to the loss of current or future customers during a 12 month period following a notification to "Us" in accordance with Section IX.A of a "Security Breach" or "Network Disruption" and where such customer loss arises directly from a "Security Breach" or "Network Disruption".

"Reputation Business Income Loss" does not include or mean:

1. any contractual penalties;

2. any costs or expenses incurred to update, upgrade, replace, restore or otherwise improve any "Computer System" to a level beyond that which existed prior to a "Network Disruption";

3. any costs or expenses incurred to identify, remove or remediate computer program errors or vulnerabilities, or costs to update, upgrade, replace, restore, maintain or otherwise improve any “Computer System”;

4. any legal costs, expenses or other amounts arising out of liability to any third party;

5. any amounts incurred as a result of unfavorable business conditions; or

6. any other consequential amounts, loss or damage.

“Restoration Costs” means the actual, reasonable and necessary costs, including the additional cost of employing temporary staff or paying overtime costs to employees, that “You” incur to replace, restore, or re-create “Your” “Digital Assets” to the level or condition at which they existed immediately prior to sustaining any alteration, destruction, damage or loss thereof, resulting from a "Security Compromise". If such “Digital Assets” cannot be replaced, restored or re-created, then “Restoration Costs” will be limited to the actual, reasonable and necessary costs “You” incur to reach this determination.

“Restoration Costs” also means the actual, reasonable and necessary costs to install a more secure and efficient version of "Your" affected "Computer System", provided that the maximum amount "We" will pay is twenty-five percent (25%) more than the cost that would have been incurred to replace the original model(s) or license(s) that existed prior to the "Security Compromise" (and subject to the maximum sublimit as stated in ITEM 3.III.H. of the Declarations). Under no circumstances will "We" pay the cost of acquiring or installing "Computer Systems" which did not form a part of "Your" "Computer Systems" immediately prior to the incident which gave rise to the "Loss".

“Restoration Costs” do not include:

1. "Systems Integrity Restoration Loss";

2. the economic or market value of any “Digital Assets”, including trade secrets.

“Retroactive Date” means the date specified in ITEM 7. of the Declarations.

"Reward Fund Loss" any amount offered and paid by "You" for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act associated with an "Event". The most “We” will pay for any “Reward Fund Loss” is the sublimit of liability stated in ITEM 3.II.I.3. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

“Security Breach” means the actual or reasonably suspected:

1. loss or disclosure of “Private Information” in “Your” care, custody or control, including such information stored on paper or on a “Computer System” operated by “You” or on “Your” behalf; or

2. “Theft of Data”, “Unauthorized Access” to or “Unauthorized Use” of “Private Information” in “Your” care, custody or control, including such information stored on paper or on a “Computer System” operated by “You” or on “Your” behalf;

that results in or may result in the compromise of the privacy or confidentiality of “Private Information”.

More than one “Security Breach” arising from the same or a series of continuous, repeated or related acts, errors, or omissions shall be considered a single “Security Breach”, which shall be deemed to have first occurred at the time of the first such “Security Breach”.

“Security Compromise” means the actual or reasonably suspected:

1. “Unauthorized Access” or “Unauthorized Use” of “Your” “Computer System” or “Your” “Digital Assets”;

2. unauthorized transmission of computer code into “Your” “Computer System” that causes loss or damage to “Your” “Digital Assets”; or

3. “Denial of Service Attack” on “Your” “Computer System” that causes loss or damage to “Your” “Digital Assets”.

“Security Wrongful Act” means any act, error, or omission committed by “You” or a person or entity for which “You” are legally responsible, including an independent contractor or outsourcing organization, in the conduct of “Computer Systems” security and the protection of the security and confidentiality of “Private Information”, that results in:

1. the inability of a third (3rd) party, who is authorized to do so, to gain access to “Your” “Computer Systems”;

2. the failure to prevent or hinder “Unauthorized Access” to or “Unauthorized Use” of a “Computer System” operated by “You” or on “Your” behalf, the failure to prevent physical theft of hardware or firmware “You” control, the failure to prevent people or processes security failures, or the failure to prevent false communications designed to trick the user into surrendering “Private Information” (such as phishing, pharming or vishing), any of which results in:

    a. The alteration, copying, corruption, destruction or deletion of, or damage to, electronic data on a “Computer System” operated by “You” or on “Your” behalf;

    b. Unauthorized disclosure of “Private Information”;

    c. “Theft of Data” (including identity theft); or

    d. Denial of service attacks against “Internet” sites or “Computer Systems” of a third (3rd) party; or

3. the failure to prevent transmission of “Malicious Code” from a “Computer System” operated by “You” or on “Your” behalf to a third (3rd) party’s “Computer System”.

"Services Fraud Event" means the unauthorized use of or access to "Your" "Computer System" by a third party which results in increased service charges to "You", including: the unauthorized use of "Your" "Computer System" by a third party to mine cryptocurrency or any other digital or electronic currency; the fraudulent or unauthorized use of Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Network-as-a-Service (NaaS), or IP Telephony.

"Services Fraud Loss" means monetary or other financial asset loss as a result of a "Services Fraud Event", provided: (1) the service provider charges "You" via a periodic billing statement pursuant to a written contract that was executed before the “Services Fraud Event” occurred; (2) the service provider charges "You" a fee that scales with the rate of use of such services; and (3) the "Services Fraud Event" began on or after the “Retroactive Date”. The most “We” will pay for any “Services

Fraud Loss" is the sublimit of liability stated in ITEM 3.II.I.2. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

"Service Provider" means any third (3rd) party that is responsible for the processing, maintenance, protection or storage of "Digital Assets" pursuant to a written contract directly with "Your Organization". A "Service Provider" does not include any provider of telecommunications services, including "Internet" access, to "You".

"Subsidiary" means any corporation of which more than fifty percent (50%) of the outstanding securities representing the present right to vote for the election of such corporation's directors are owned by the "Named Insured" directly or indirectly, if such corporation was so owned on the inception date of this Policy; or

1. becomes so owned after the inception date of this Policy, provided the revenues of the newly acquired corporation do not exceed twenty-five percent (25%) of "Your Organization's" annual revenues as set forth in its most recent audited financial statement; or

2. becomes so owned after the inception date of this Policy, provided that if the revenues of the newly acquired corporation exceed twenty-five percent 25%) of "Your Organization's" annual revenues as set forth in its most recent audited financial statement, the provisions of Section IX. I. must be fulfilled.

"Systems Integrity Restoration Loss" means the reasonable and necessary costs "You" incur, with our prior written consent, to restore or replace that part of "Your" "Computer System" directly impacted by a "Security Compromise". "System Integrity Restoration Loss" does not include "Restoration Costs". The most "We" will pay for any "Systems Integrity Restoration Loss" is the sublimit of liability stated in ITEM 3.II.G.4. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage G and not in addition.

"Telecommunications Services" means telephone, fax, broadband, or other data transmission services that "Your Organization" purchases from third parties.

"Telephone Hacking Event" means a third party's intentional, unauthorized and fraudulent use of "Your" "Telecommunications Services" that results in unauthorized calls or unauthorized use of "Your" bandwidth.

"Telephone Hacking Loss" means "Your" monetary or other financial asset loss as a result of a "Telephone Hacking Event". The most "We" will pay for any "Telephone Hacking Loss" is the sublimit of liability stated in ITEM 3.II.I.6. of the Declarations. Such sublimit is part of the Limit of Liability in Coverage I and not in addition.

"Theft Of Data" means the unauthorized taking, misuse or disclosure of information on including but not limited to charge, debit, or credit information, banking, financial and investment services account information, proprietary information, and "Private Information".

"Unauthorized Access" means the gaining of access to a "Computer System" by an unauthorized person or an authorized person in an unauthorized manner.

"Unauthorized Use" means the use of a "Computer System" by an unauthorized person or an authorized person in an unauthorized manner.

"Waiting Period" means the time period specified in ITEM 11. of the Declarations.

"We", "Us" or "Our" means the underwriters providing this insurance.

"Wrongful Act" means a "Privacy Wrongful Act", "Security Wrongful Act", "Multimedia Wrongful Act", or "PCI DSS Wrongful Act".

"You" or "Your" or "Yours" means:

1. the entity named in ITEM 1. of the Declarations ("Named Insured") and its "Subsidiaries" (together "Your Organization");

2. any present or future director, officer, or trustee of "Your Organization", but only with respect to the performance of his or her duties as such on behalf of "Your Organization";

3. any present or future "Employee" of "Your Organization" but only with respect to work done while acting within the scope of his or her employment and related to the conduct of "Your Organization's" business;

4. in the event that the "Named Insured" is a partnership, limited liability partnership, or limited liability company, then any general or managing partner, principal, or owner thereof, but only while acting within the scope of his or her duties as such;

5. any person who previously qualified as "You" under 2, 3, or 4 above prior to the termination of the required relationship with "Your Organization", but only with respect to the performance of his or her duties as such on behalf of "Your Organization";

6. the estate, heirs, executors, administrators, assigns and legal representatives of any of "You" in the event of "Your" death, incapacity, insolvency or bankruptcy, but only to the extent that "You" would otherwise be provided coverage under this insurance;

7. any agent or independent contractor, including any distributor, licensee or sub-licensee, but only while acting on "Your" behalf, at "Your" direction, and under "Your" control; and

8. any third (3rd) party entity (including a HIPAA Covered Entity) required by contract to be named as an insured under this Policy, but only in respect of sums which they become legally obligated to pay (including liability for claimants' costs and expenses) as a result of a "Claim" arising solely out of an act, error or omission committed by "You", provided that:

   a) "You" contracted in writing to indemnify the third (3rd) party for such a "Claim" prior to it first being made against them; and

   b) had the "Claim" been made against "You", then "You" would be entitled to indemnity under this Policy.

   As a condition to "Our" indemnification of any third (3rd) party they shall prove to "Our" satisfaction that the "Claim" arose solely out of a "Wrongful Act", act, error or omission committed by "You"; and where a third (3rd) party is indemnified as an additional insured as a result, it is understood and agreed that any "Claim" made by that third (3rd) party against "You" shall be treated by "Us" as if they were a third (3rd) party, not an additional insured.

## VI. LIMITS OF LIABILITY

Limits of Liability for Damages and Claims Expenses

A. The amount stated in the Policy as stated in ITEM 3.I of the Declarations (herein the "Policy Aggregate Limit") is the most "We" will pay in the aggregate under this Policy, under all Coverages combined, for:

1. all “Damages”; and

2. all “Claims Expenses**”**.

regardless of the number of “Claims”, “Events”, “Wrongful Acts”, acts, errors, or omissions, insured persons, insured entities or claimants involved, or Coverages triggered.

B. For any Coverage purchased as indicated in ITEM 3.II of the Declarations, any Per Single “Claim”, Per Single “Event” or Aggregate Per Coverage “Sublimit(s) of Liability” shall be part of, and not in addition to, the “Policy Aggregate Limit”, unless otherwise specified.

C. If any single “Claim”, single “Event”, or single “Event” combined with a single “Claim” directly arising therefrom (“Combined Matter”) is covered under more than one Coverage, the highest applicable Per Single “Claim” or Per Single “Event” “Sublimit of Liability” shall be the most “We” shall pay as to such single “Claim”, single “Event” or “Combined Matter”, and such single “Claim”, single “Event” or “Combined Matter” shall be subject to the highest applicable retention, unless otherwise specified.

D. Any Aggregate Per Coverage “Sublimit of Liability” as stated in ITEM 3.II of the Declarations shall be the most “We” will pay in the aggregate for any given Coverage, for:

1. all “Damages”; and
2. all “Claims Expenses**”.**

regardless of the number of “Claims”, “Events”, “Wrongful Acts”, acts, errors, or omissions, insured persons, insured entities or claimants to which such given Coverage applies.

Limits of Liability for Loss(es)

E. The amount stated in the Policy as stated in ITEM 3.I of the Declarations (herein the “Each Event Aggregate Limit”) is the most “We” will pay in the aggregate under this Policy for all "Loss" arising out of a single "Event".

F. Any Aggregate Per Coverage “Sublimit of Liability” as stated in ITEM 3.II of the Declarations shall be the most “We” will pay in the aggregate for any given Coverage under this Policy for all "Loss" arising out of a single "Event".

## VII. RETENTIONS

The retention for each Coverage is stated in ITEM 4 of the Declarations. The applicable retention shall be first applied to “Damages”, “Claims Expenses” and “Loss” covered by this Policy and “You” shall make direct payments within the retention to appropriate other parties designated by “Us”. “We” shall be liable only for the amounts in excess of the retention, not to exceed the applicable “Sublimit(s) of Liability” or “Policy Aggregate Limit”. Each single “Claim”, single “Event” or “Combined Matter” shall be deemed to be one single potentially covered matter, and only one retention shall apply thereto. Where multiple Coverages potentially apply to a single “Claim”, single “Event” or “Combined Matter”; only one retention shall apply and this shall be the highest retention applicable to such Coverages.

Except as otherwise provided, the amount set forth in ITEM 4 of the Declarations (the "Aggregate Retention Amount") is the most "You" will pay for all retentions combined under this Policy regardless of the number of "Claims", "Events", or "Wrongful Acts". Upon payment of the "Aggregate Retention Amount" by "You" the applicable retentions shall be waived.

No retention is applicable to “Breach Response Counsel” fees and expenses.

With respect to Coverage G. 1, once the "Period of Restoration" has exceeded the "Waiting Period", the retention stated in ITEM 4 of the Declarations shall be applied against the "Business Income Loss" computed from the commencement of the "Network Disruption".

At "Our" sole and absolute discretion, "We" may pay all or part of the applicable retention, in which case "You" agree to repay "Us" immediately after "We" notify "You" of the payment; and such payment or repayment of any amount within the retention shall be first applied to "Damages", "Claims Expenses" and "Loss" covered by this Policy.

## VIII. EXTENDED REPORTING PERIOD

A. Basic "Extended Reporting Period": In the event of cancellation or non-renewal of this Policy by "You" or "Us", an "Extended Reporting Period" of sixty (60) days immediately following such cancellation or non-renewal shall be automatically granted hereunder at no additional premium. Such "Extended Reporting Period" shall cover "Claims" first made and reported to "Us" during such sixty (60) day "Extended Reporting Period" but only in respect of any act, error, or omission committed prior to the date of cancellation or non-renewal, and subject to all other terms, conditions, and exclusions of this Policy. No "Claim" in such sixty (60) day extended reported period shall be covered under this Policy if "You" are entitled to indemnity under any other insurance or would have been entitled to indemnity under such insurance but for the exhaustion thereof.

B. Optional "Extended Reporting Period": In the event of cancellation or non-renewal of this Policy by "You" or "Us", "You" shall have the right, upon payment in full and not proportionally or otherwise in part to have issued an endorsement providing an optional "Extended Reporting Period" after the end of the "Policy Period" as follows.

| **Extended Reporting Period** | **Extended Reporting Period Premium** |
|---|---|
| 12 Months | 100% of the Annual Policy Premium |
| 24 Months | 150% of the Annual Policy Premium |
| 36 Months | 200% of the Annual Policy Premium |

C.

1. Such optional "Extended Reporting Period" shall cover "Claims" made and reported to "Us" during this optional "Extended Reporting Period", but only in respect of any "Claim" arising out of any act, error, or omission committed prior to the date of cancellation or non-renewal, and subject to all other terms, conditions, and exclusions of the Policy.

2. In order for "You" to invoke the optional "Extended Reporting Period", the payment of additional premium as stated in this provision must be paid to "Us" within sixty (60) days after the end of the "Policy Period".

3. At the commencement of the optional "Extended Reporting Period", the entire premium shall be deemed fully earned, and in the event "You" terminate the optional "Extended Reporting Period" for whatever reason prior to its natural expiration, "We" will not be liable to return any premium paid for the optional "Extended Reporting Period".

D. Terms and conditions of basic and optional "Extended Reporting Period":

1. At renewal of this Policy, "Our" quotation of different premium, retention or limit of indemnity or changes in policy language shall not constitute non-renewal by "Us" for the purposes of granting the optional "Extended Reporting Period".
2. The right to the "Extended Reporting Period" shall not be available to "You" where "We" cancel or non-renew due to non-payment of premium.
3. The limit of liability for the "Extended Reporting Period" shall be part of, and not in addition to, the limit of liability for the "Policy Period".

4. All notices and premium payments with respect to the “Extended Reporting Period” shall be directed to “Us” through the entity named in the Policy.

## IX. TERMS AND CONDITIONS

### A. NOTICE OF CLAIM OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM

1. If any “Claim” is made against “You” during the “Policy Period” (or an “Extended Reporting Period”, if applicable), or an “Event” first occurs during the “Policy Period”, then as soon as practicable after a member of the “Control Group” becomes aware of such “Claim” or “Event”, “You” must provide notice thereof to “Us” through the person identified in ITEM 8. in the Declarations, during the “Policy Period” (or an “Extended Reporting Period”, if applicable), including every demand, notice, summons or other process “You” or “Your” representative receive.

2. If during the “Policy Period” a member of the “Control Group” becomes aware of any situation, circumstance, “Wrongful Act”, act, error or omission that might reasonably give rise to a “Claim”, and if “You” give written notice to “Us” through the person identified in ITEM 8. in the Declarations, as soon as practicable during the “Policy Period”, of:

   a. The specific details of the situation, circumstance, “Wrongful Act”, act, error or omission that might reasonably give rise to a “Claim”;

   b. The possible damage which may result or has resulted from the situation, circumstance, “Wrongful Act”, act, error or omission;

   c. A description of how “You” first became aware of the situation, circumstance, “Wrongful Act”, act, error or omission; and

   d. Any “Computer System” security and event logs which provide evidence of the situation, circumstance, “Wrongful Act”, act, error or omission,

   then any subsequent “Claim” made against “You” arising out of such situation, circumstance, “Wrongful Act”, act, error or omission which is the subject of the written notice will be deemed to have been first made at the time written notice complying with the above requirements was first given to “Us”.

3. A “Claim” shall be considered to be reported to “Us” when notice is first given to “Us” through the person identified in ITEM 8. in the Declarations or when notice of a situation, circumstance, “Wrongful Act", act, error or omission which might reasonably give rise to a “Claim” is first provided in compliance with Section IX.A.2 above. An “Event” shall be considered reported to “Us” when notice is first given to “Us” through the person identified in ITEM 8. in the Declarations.

4. Whenever coverage under this Policy would be lost due to non-compliance of Section IX.A.1.’s notice requirements because of the failure to give such notice, or concealment of such failure, by one or more “You” responsible for causing the “Damage”, “Loss” or other amounts potentially insured hereunder, then “We” agree that such insurance as would otherwise be afforded under this Policy shall remain available with respect to those of “You” who did not personally commit, personally participate in committing or personally acquiesce in such failure to give notice, provided that those of “You” entitled to the benefit of this provision provide notice of a “Claim” or “Event” during the “Policy Period” (or “Extended Reporting Period”, if applicable), promptly after obtaining knowledge of such failure of any others of “You” to comply with Section IX.A.1.

However, such insurance as afforded by this provision shall not cover a “Claim” against “Your Organization”, or an “Event”, if a member of the “Control Group” failed to give notice as required by Section IX.A.1.if such “Claim” or “Event” arises from “Wrongful Acts”, acts, errors or omissions that were also known to another then current member of the “Control Group”.

**B. ASSISTANCE AND COOPERATION**

1. “You” shall cooperate with “Us” in all investigations. “You” shall execute or cause to be executed all papers and render all assistance as requested by “Us”. Part of this assistance may require “You” to provide soft copies of “Your” system security and event logs.

2. Upon “Our” request, “You” 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 “You” because of “Wrongful Acts”, acts, errors, or omissions with respect to which insurance is afforded under this Policy; and “You” shall attend hearings and trials and assist in securing and giving evidence and obtaining the attendance of witnesses.

3. “You” shall not admit liability, make any payment, assume any obligation, incur any expense, enter into any settlement, stipulate to any judgment or award or dispose of any “Claim” without “Our” written consent, unless otherwise provided under Section II.

4. As soon as practicable after “You” give “Us” notice of any “Claim”, “Event”, or circumstance, “You” must also give “Us” copies of reports, photographs, investigations, pleadings and all other papers in connection therewith, including allowing “Us” to question “You” under oath at such times as may be reasonably required regarding “Your Organization’s” books, records, and any other information relating to such matters.

5. In the event of a “Privacy Breach”, “Security Breach” or other “Event”, “You” must take all reasonable steps to protect “Computer Systems” and “Private Information” from further access, disclosure, loss or damage.

**C. DUTIES FOLLOWING NOTICE OF AN EVENT (applicable to Coverages C, F, G and I only).**

“You” must see that the following are done if “You” send “Us” notice of an “Event” to which Coverages C, F, G or I potentially apply:

1. at “Our” request, notify the police, FBI, CERT or other applicable law enforcement authority, central reporting or investigative organization that “We” may designate, if it appears that a law may have been broken;

2. immediately take all reasonable steps and measures necessary to limit or mitigate the “Loss”;

3. send “Us” copies of every demand, notice, summons, or any other applicable information “You” receive;

4. if requested, permit “Us” to question “You” under oath at such times and places as may be reasonably required about matters relating to this insurance, including “Your” books and records;

5. send “Us” a sworn statement of “Loss” or other amounts incurred containing the information “We” request to resolve, settle or otherwise handle the “Event”. “We” will provide “You” with the necessary forms;

6. cooperate with “Us” and counsel “We” may appoint in the investigation of any “Event” covered by this Policy;

7. assist “Us” and counsel “We” may appoint in the investigation or settlement of “Loss”;

8. assist “Us” in protecting and enforcing any right of subrogation, contribution or indemnity against any person, organization or other entity that may be liable to “You”, including attending depositions, hearings and trials;

9. assist “Us” when a “Telephone Hacking Event” and/or “Funds Transfer Fraud” occurs, and

10. otherwise assist in securing and giving documentation and evidence, and obtaining the attendance of witnesses.

    A “Telephone Hacking Event” will be deemed to occur when “You” first discover that a “Telephone Hacking Event” has occurred, or “You” have a reasonable basis to know that a “Telephone Hacking Event” has occurred, including the receipt of any notice, invoice, or billing evidencing unauthorized use of “Telecommunications Services”. If any related “Telephone Hacking Events” subsequently occur, and are reported to “Us,” all such related “Telephone Hacking Events” will be considered a single “Telephone Hacking Event” and will be deemed to have occurred on the date the first of those “Telephone Hacking Events” occurred.

    “Funds Transfer Fraud” will be deemed to occur when “You” first know that a “Funds Transfer Fraud” has occurred, or “You” have a reasonable basis to know that a “Funds Transfer Fraud” has occurred, including any unauthorized electronic funds transfer; theft of “Your” money or other financial assets from "Your" bank by electronic means; theft of money or other financial assets from “Your” corporate credit cards by electronic means; or any fraudulent manipulation of electronic documentation while stored on “Your” “Computer System”. If related “Funds Transfer Fraud” events subsequently occur, and are reported to “Us,” all such related “Funds Transfer Fraud” events will be considered a single “Funds Transfer Fraud” event and will be deemed to have occurred on the date the first of those “Funds Transfer Fraud” events occurred.

    As soon as a “Telephone Hacking Event” and/or “Funds Transfer Fraud” first occurs, “You” must notify us in accordance with Section IX., TERMS AND CONDITIONS, paragraph A. NOTICE OF CLAIM OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM.

**D. SUBROGATION**

In the event of any payment under this Policy, “You” agree to give “Us” the right to any subrogation and recovery to the extent of “Our” payments. “You” agree to execute all papers required and will do everything that is reasonably necessary to secure these rights to enable “Us” to bring suit in “Your” name. “You” agree to fully cooperate in “Our” prosecution of that suit. “You” agree not to take any action that could impair “Our” right of subrogation without “Our” written consent, whether or not “You” have incurred any unreimbursed amounts. Any recoveries shall be applied first to subrogation expenses, second to “Damages”, “Claims Expenses” and “Loss” paid by “Us”, and third to the Retention. Any additional amounts recovered shall be paid to “You”.

**E. INSPECTIONS AND SURVEYS**

“We” may choose to perform inspections or surveys of “Your” operations, conduct interviews and review documents as part of “Our” underwriting, “Our” decision whether to provide continued or modified coverage, or “Our” processing of any “Claim” or “Event”. If “We” make recommendations as a result of these inspections, “You” should not assume that every possible recommendation has been made or that “Your” implementation of a recommendation will prevent a “Claim” or “Event”. “We” do not indicate by making an inspection or by providing “You” with a report that “You” are complying with or violating any laws, regulations, codes or standards.

## F. OTHER INSURANCE

This insurance shall apply in excess of any other valid and collectible insurance available to "You", including any retention or deductible portion thereof, unless such other insurance is written only as specific excess insurance over this Policy. However, this insurance shall apply as primary in respect of any directors & officers, professional liability, errors & omissions, medical malpractice or professional service liability policy purchased by "You".

## G. ACTION AGAINST US

No action shall lie against "Us" or "Our" representatives unless, as a condition precedent thereto: (1) there shall have been full compliance with all terms of this insurance; and (2) until the amount of "Your" obligation to pay shall have been finally determined by judgment or award against "You" after trial, regulatory proceeding, or arbitration or by written agreement between "You", the claimant, and "Us".

"Your" bankruptcy or insolvency shall not relieve "Us" of "Our" obligations hereunder.

## H. ENTIRE AGREEMENT

By acceptance of the Policy, "You" agree that this Policy embodies all agreements between "You" and "Us" relating to this insurance. 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 stop "Us" from asserting any right under the terms of this Policy; nor shall the terms of this Policy be waived or changed, except by endorsement issued to form a part of this Policy signed by "Us".

## I. NEW SUBSIDIARIES/CHANGES IN NAMED INSURED OR YOUR ORGANIZATION

1. During the "Policy Period", if "You" acquire another corporation whose annual revenues are more than twenty-five percent (25%) of "Your Organization's" annual revenues as set forth in its most recent audited financial statements, "You" shall give "Us" written notice of the acquisition containing full details thereof, no later than sixty (60) days after the effective date of such acquisition or creation. Coverage under this Policy for "Wrongful Acts", acts, errors, or omissions committed or allegedly committed by the newly acquired "Subsidiary" or any persons who may become insureds therewith shall be automatic for ninety (90) days after such acquisition or creation or, until the end of the 'Policy Period,' whichever is earlier; after the end of this ninety (90) day period, "We" may agree to add coverage for the newly acquired "Subsidiary" upon such terms, conditions, and limitations of coverage and such additional premium as "We", in "Our" sole discretion, may require.

2. During the "Policy Period", if the "Named Insured" consolidates or merges with or is acquired by another entity, or sells substantially all of its assets to another entity, or a receiver, conservator, trustee, liquidator, or rehabilitator, or any similar official is appointed for or with respect to the "Named Insured", then all coverage under this Policy shall continue for post-transaction "Claims" first made prior to the expiration of the "Policy Period" but only for "Wrongful Acts", acts, errors or omissions that occurred prior to the date of such consolidation, merger or appointment. Coverage under this Policy shall not continue for "Events" that first commence post-transaction but prior to the expiration of the "Policy Period", unless coverage for such "Events" is specifically agreed to by "Us" and provided by endorsement hereto.

3. Should an entity cease to be a “Subsidiary” after the inception date of this Policy, coverage with respect to such entity and its insured persons shall continue as if it was still a “Subsidiary” until the expiration date of this Policy, but only with respect to a “Claim” that arises out of any “Wrongful Act”, act, error, or omission committed prior to the date that it ceased to be a “Subsidiary”.

4. All notices and premium payments made under this paragraph shall be directed to “Us” through the “Named Insured”.

**J. ASSIGNMENT**

“Your” interest under this Policy may not be assigned to any other person or organization, whether by operation of law or otherwise, without “Our” written consent. If “You” shall die or be adjudged incompetent, such insurance shall cover “Your**”** legal representative as “You” would be covered under this Policy.

**K. CANCELLATION AND NON-RENEWAL**

This Policy may be cancelled or non-renewed by “You” at any time on request by sending a prior written notice to “Us” stating when thereafter the cancellation will be effective.

1. “We” may not cancel this Policy, except for nonpayment of Premium. If “We” cancel this Policy for non-payment of Premium, “We” will provide “You” with at least twenty (20) days advance written notice.

2. If this Policy is cancelled by “You”, “We” shall refund the unearned Premium computed pro-rata. If this Policy is cancelled by “Us”, the refund of paid Premium shall be computed pro-rata. Payment or tender of any unearned Premium by “Us” shall not be a condition precedent to the effectiveness of such termination, but such payment shall be made as soon as practicable. No Premium will be refunded where any “Claims” or circumstances have been notified under this Policy.

3. “We” may non-renew this Policy by providing “You” with at least sixty (60) days written notice before the expiration date. If the notice is given less than sixty (60) days before expiration, Coverage will remain in effect until sixty (60) days after notice is mailed. The Premium due for any period of Coverage that extends beyond the expiration date will be determined pro-rata based upon this Policy’s total Premium for the expiring Policy Period.

4. Any offer to renew this Policy on terms involving a change in Retentions, Limit of Liability, Premium or other terms or conditions will not constitute a refusal to renew this Policy.

**L. WORDS AND TITLES OF PARAGRAPHS**

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

**M. NAMED INSURED AUTHORIZATION**

The “Named Insured” has the right and duty to act on “Your” behalf for:

1. the giving and receiving of notice of cancellation;

2. the payment of premiums, including additional premiums;

3. the receiving of any return premiums;

4. the acceptance of any endorsements added after the effective date of coverage;

5. the payment of any retentions;

6. the receiving of any amounts paid hereunder; and

7. otherwise corresponding with “Us”.

**N. REPRESENTATIONS BY YOU**

By acceptance of this Policy, “You” agree that the statements contained in the “Application”, any application for coverage of which this Policy is a renewal, and any supplemental materials submitted therewith, are “Your” agreements and representations, that they shall be deemed material to the risk assumed by “Us”, and that this Policy is issued in reliance upon the truth thereof.

The misrepresentation or non-disclosure of any matter by “You” or “Your” agent in the “Application”, any application for coverage of which this Policy is a renewal, or any supplemental materials submitted therewith will render the Policy null and void and relieve “Us” from all liability under the Policy.

**O. SERVICE OF SUIT CLAUSE (U.S.A.)**

1. It is agreed that in the event of “Our” failure to pay any amount claimed to be due under this Policy, at “Your” request “We” will submit to the jurisdiction of a court of competent jurisdiction within the United States. Nothing in this clause constitutes or should be understood to constitute a waiver of “Our” rights to commence an action in any court of competent jurisdiction in the United States, to remove an action to a United States District Court, or seek a transfer of a case to another court as permitted by the laws of the United States or any state in the United States. It is further agreed that service of process in such suit may be made upon “Our” representative, designated in the Policy, and that in any suit instituted against any one of “Us” upon this contract, “We” will abide by the final decision of such court or of any appellate court, in the event of an appeal.

2. “Our” representative designated in the Policy is authorized and directed to accept service of process on “Our” behalf in any such suit and/or upon “Your” request to give a written undertaking to “You” that they will enter a general appearance upon “Our” behalf in the event such a suit shall be instituted.

3. Pursuant to any statute of any state, territory, or district of the United States which makes provision therefore, “We” hereby designate the Superintendent, Commissioner, or Director of Insurance or other officer specified for that purpose in the statute, or his successor in office, as “Our” true and lawful attorney upon whom may be served any lawful process in any action, suit, or proceeding instituted by or on behalf of “You” or any beneficiary hereunder arising out of this Policy, and hereby designate “Our” representative listed in the Policy as the person to whom the said officer is authorized to mail such process or a true copy thereof.

**P. CHOICE OF LAW**

Any disputes involving this Policy shall be resolved applying the laws of the state identified in ITEM 10. of the Declarations.

**Q. ARBITRATION**

Any controversy arising out of or relating to this policy or the breach, termination or invalidity thereof shall be settled by binding arbitration in accordance with the commercial arbitration rules, but not the authority or jurisdiction, of the American Arbitration Association (herein “AAA”) then in effect. “We**”** and the "Named Insured" shall each appoint an arbitrator. Each arbitrator must be disinterested other than the "Named Insured" or any present or former officers or directors of the Insured. As soon as one party notifies the other of its demand for arbitration and names its arbitrator, the other party agrees to name its arbitrator within thirty (30) days of said notice. Within thirty (30) days of the naming of the second arbitrator, the two arbitrators will select a third arbitrator to be chairman of the panel, other than the "Named Insured" or any present or former officers or directors of the Insured. Should the two arbitrators not be able to agree on a choice of the third, then the Chief Judge of the chosen competent jurisdiction will make the appointment of such third arbitrator. None of the arbitrators may be current or former officers, directors, or employees of the "Named Insured" or “Us.” The three arbitrators will comprise the arbitration panel for the purposes of this Policy.

Each party to this policy will submit its case with supporting documents to the arbitration panel within thirty (30) days after appointment of the third arbitrator. However, the panel may agree to extend this period for a reasonable time. Unless extended by the consent of the parties, the majority of the three arbitrators will issue a written decision resolving the controversy before them within thirty (30) days of the time the parties are required to submit their cases and related documentation. The arbitrators’ written decision will state the facts reviewed, conclusions reached and the reasons for these conclusions. That decision will be final and binding upon the parties in any court of competent jurisdiction.

Each party will pay the fees and expenses of its arbitrator, unless otherwise agreed by the parties. The remaining costs of arbitration will be shared equally by the parties.

Arbitration will take place in a competent jurisdiction agreed to by the parties.

Any disputes involving this Policy shall be resolved applying the substantive law as designated in ITEM 10. of the Declarations.

In witness whereof, the company has caused this policy to be signed by its President and its Secretary at Oakbrook Terrace, Illinois.

PRESIDENT SECRETARY

BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

# CYBER DECEPTION ENDORSEMENT - CONNECTICUT

## CYBER AND PRIVACY LIABILITY POLICY

94.510 CT (07/19)

This Endorsement, effective at 12:01 a.m. CST, on March 18, 2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

Issued by: BCS Insurance Company

**Retention:** The retention for a "Loss" resulting from a "Cyber Deception Event" is as stated in ITEM 4.I.8 of the Declarations. A single retention shall apply to a "Cyber Deception Event" arising out of the same, related, or continuing acts, facts, or circumstances.

**Sublimit:** The most "We" will pay for a "Loss" resulting from a "Cyber Deception Event" is the amount stated in ITEM 3.II.I.8 of the Declarations. Such sub-limit shall be part of and not in addition to the "Policy Aggregate Limit".

If a "Cyber Deception Event" arises from the same or a series of related or repeated acts, errors, or omissions or from any continuing acts, errors, or omissions, this shall be considered a single "Event" for the purposes of this policy and each corresponding retention shall apply separately to the applicable portion of such single "Event". In no event shall the corresponding retentions be combined to create a larger retention amount than that exists for each corresponding retention.

This Endorsement modifies insurance provided under the following:

**CYBER AND PRIVACY LIABILITY POLICY**

In consideration of the premium required for the Cyber Deception Endorsement, and subject to all of the terms, conditions and exclusions in the Policy referenced above, (except as amended by this Endorsement), the Company hereby agrees to extend coverage to the Insured as follows:

**CYBER DECEPTION**

“We” shall reimburse "Your Organization" for the "Loss of Funds" or for the "Value of Goods" transferred which occur as a direct result of a "Cyber Deception Event" (which follows the "Retroactive Date" on the Declarations) which is notified to "Us" during the "Policy Period".

**A. DEFINITIONS:**

"Account" means any bank account held in the name of "Your Organization" or value stored in the form of cryptocurrency;

"Client" means any individual or entity to whom "You" are contracted to perform services or supply goods;

"Cyber Deception" means the intentional misleading of "You" by means of a dishonest misrepresentation of a material fact contained or conveyed within an electronic or telephonic communication(s) and which relied upon by "You" believing it to be genuine.

"Cyber Deception Event" means:

1. The good faith transfer by "You" of "Your Organization's" funds or the transfer of "Your Goods", in lieu of payment, to a third party as a direct result of a "Cyber Deception", whereby "You" were directed to transfer "Goods" or pay funds to a third party under false pretenses; or

2. The theft of "Your Organization's" funds as a result of an unauthorized intrusion into or "Security Compromise" of "Your" "Computer System" directly enabled as a result of a "Cyber Deception".

Solely with respect to this Endorsement, the definition of "Event" is amended to include a "Cyber Deception Event".

"Goods" means those products supplied by "You" to a "Client" under a contract.

"Loss of Funds" means the loss of money from "Your" "Account", or the loss of money held on behalf of "Your" customers or clients. "Loss of Funds" shall not include:

1. Any fees, fines or charges assessed against "You" or any expenses "You" incur as a result of any "Cyber Deception Event"; or

2. The cost of "Your" time in identifying and rectifying the "Cyber Deception Event".

Solely with respect to this Endorsement, the definition of "Loss" is amended to include "Loss of Funds".

"Value of Goods" means the cost price of those "Goods" excluding:

1. Any element of profit to "Your Organization"; or

2. Any tax which "You" may be able to recover as a result of "Goods" being misappropriated by way of the "Cyber Deception Event".

Solely with respect to this Endorsement, the definition of "Loss" is amended to include the "Value of Goods".

**B. NOTICE OF CYBER DECEPTION EVENT**

If any "Cyber Deception Event" occurs, then as soon as reasonably practicable after "Your" Chief Executive Office, Finance Director, General Counsel, or Risk Manager or their functional equivalents becomes aware of such "Cyber Deception Event", "You" shall notify "Us" by forwarding notice to the persons named in Item 8. of the Declarations and giving as much details as possible of the following:

1. Specific details of the acts, facts, or circumstances that gave rise to the "Cyber Deception Event";

2. Possible amounts potentially covered under this policy that may result or have resulted from the acts, facts or circumstances;

3. Details regarding how "You" first became aware of the acts, facts, or circumstances; and

4. The "Computer Network" security and event logs, which provide evidence of the alleged incident.

Any subsequent "Cyber Deception Event" arising out of such acts, facts, or circumstances which is the subject of the written notice will be deemed to be a "Cyber Deception Event" at the time written notice complying with the above requirements was first given to "Us".

**C. EXCLUSIONS**

"We" shall not be liable for any "Cyber Deception Event" arising out of:

1. Any "Cyber Deception Event", which was first committed or occurred prior to the "Retroactive Date";

2. Any "Cyber Deception Event" notified to and accepted by a previous insurer under an insurance policy of which this policy is a renewal or replacement;

3. Any "Loss of Funds" or "Value of Goods" arising out of or caused by:

   a. The wear and tear, drop in performance, progressive or gradual deterioration, or aging of electronic equipment and other property or "Hardware" used by "You";

   b. Failure by "You" or those acting on "Your" behalf to maintain any computer, computer network or network, computer software, or any other equipment;

   c. Failure or gradual deterioration of overhead transmission, distribution lines or subterranean insulation or cabling;

   d. "Your" knowing use of illegal or unlicensed programs that are in violation of provisions or laws referring to software protection; or

   e. 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.

4. Gambling, pornography, prizes, awards, coupons, or the sale or provision of prohibited, restricted, or regulated items including, but not limited to, alcoholic beverages, tobacco, or drugs.

**D. CANCELLATION AND NONRENEWAL**

“You” may not cancel the coverage afforded by this Endorsement unless “You” cancel this entire Policy pursuant to Section IX. K. of this Policy, in which case the entire premium paid for this Endorsement shall be fully earned and non-refundable if notice of any “Cyber Deception Event” or other circumstances actually or potentially covered under this Endorsement has been given to “Us”.

**BCS Insurance Company**
**2 Mid America Plaza, Suite 200**
**Oakbrook Terrace, IL 60181**
**(312) 803-7384**

# CONNECTICUT NUCLEAR INCIDENT EXCLUSION CLAUSE-LIABILITY-DIRECT (BROAD) (U.S.A.)

94.102 CT (01/15)

---

This Endorsement, effective at 12:01 a.m. CST, on March 18, 2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

Issued by: BCS Insurance Company

For attachment to insurances of the following classifications in the U.S.A., its Territories and Possessions, Puerto Rico and the Canal Zone:

> Owners, Landlords and Tenants Liability, Contractual Liability, Elevator Liability, Owners or Contractors (including railroad) Protective Liability, Manufacturers and Contractors Liability, Product Liability, Professional and Malpractice Liability, Storekeepers Liability, Garage Liability, Automobile Liability (including Massachusetts Motor Vehicle or Garage Liability),

not being insurances of the classifications to which the Nuclear Incident Exclusion Clause-Liability-Direct (Limited) applies.

This Policy* does not apply:

I. Under any Liability Coverage, to injury, sickness, disease, death or destruction:

(a) with respect to which an insured under the Policy is also an insured under a nuclear energy liability policy issued by Nuclear Energy Liability Insurance Association, Mutual Atomic Energy Liability Underwriters or Nuclear Insurance Association of Canada, or would be an insured under any such policy but for its termination upon exhaustion of its limit of liability; or

(b) resulting from the hazardous properties of nuclear material and with respect to which (1) any person or organization is required to maintain financial protection pursuant to the Atomic Energy Act of 1954, or any law amendatory thereof, or (2) the insured is, or had this Policy not been issued would be, entitled to indemnity from the United States of America, or any agency thereof, under any agreement entered into by the United States of America, or any agency thereof, with any person or organization.

II. Under any Medical Payments Coverage, or under any Supplementary Payments Provision relating to immediate medical or surgical relief, to expenses incurred with respect to bodily injury, sickness, disease or death resulting from the hazardous properties of nuclear material and arising out of the operation of a nuclear facility by any person or organization.

III. Under any Liability Coverage, to injury, sickness, disease, death or destruction resulting from the hazardous properties of nuclear material, if:

(a) the nuclear material (1) is at any nuclear facility owned by, or operated by or on behalf of, an insured or (2) has been discharged or dispersed therefrom;

(b) the nuclear material is contained in spent fuel or waste at any time possessed, handled, used, processed, stored, transported or disposed of by or on behalf of an insured; or

(c) the injury, sickness, disease, death or destruction arises out of the furnishing by an insured of services, materials, parts or equipment in connection with the planning, construction, maintenance, operation or use of any nuclear facility, but if such facility is located within the United States of America, its territories or possessions or Canada, this exclusion (c) applies only to injury to or destruction of property at such nuclear facility.

IV. As used in this endorsement:

"hazardous properties" include radioactive, toxic or explosive properties; "nuclear material" means source material, special nuclear material or by-product material; "source material", "special nuclear material", and "by-product material" have the meanings given them in the Atomic Energy Act 1954 or in any law amendatory thereof; "spent fuel" means any fuel element or fuel component, solid or liquid, which has been used or exposed to radiation in a nuclear reactor; "waste" means any waste material (1) containing by-product material and (2) resulting from the operation by any person or organization of any nuclear facility included within the definition of nuclear facility under paragraph (a) or (b) thereof; "nuclear facility" means:

(a) any nuclear reactor,
(b) any equipment or device designed or used for (1) separating the isotopes of uranium or plutonium, (2) processing or utilizing spent fuel, or (3) handling, processing or packaging waste,
(c) any equipment or device used for the processing, fabricating or alloying of special nuclear material if at any time the total amount of such material in the custody of the insured at the premises where such equipment or device is located consists of or contains more than 25 grams of plutonium or uranium 233 or any combination thereof, or more than 250 grams of uranium 235,
(d) any structure, basin, excavation, premises or place prepared or used for the storage or disposal of waste, and includes the site on which any of the foregoing is located, all operations conducted on such site and all premises used for such operations; "nuclear reactor" means any apparatus designed or used to sustain nuclear fission in a self-supporting chain reaction or to contain a critical mass of fissionable material. With respect to injury to or destruction of property, the word "injury" or "destruction" includes all forms of radioactive contamination of property.

NOTE: As respects policies which afford liability coverages and other forms of coverage in addition, the words underlined should be amended to designate the liability coverage to which this clause is to apply.

It is understood and agreed that, except as specifically provided in the foregoing to the contrary, this clause is subject to the terms, exclusions, conditions and limitations of the Policy to which it is attached.

**BCS Insurance Company**
**2 Mid America Plaza, Suite 200**
**Oakbrook Terrace, IL 60181**
**(312) 803-7384**

# RADIOACTIVE CONTAMINATION EXCLUSION CLAUSE-LIABILITY DIRECT (U.S.A.)

94.103 01/15

---

This Endorsement, effective at 12:01 a.m. CST, on March 18, 2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

Issued by: BCS Insurance Company

When attached to the Policy, (in addition to the appropriate Nuclear Incident Exclusion Clause-Liability-Direct) provides worldwide coverage.

In relation to liability arising outside the U.S.A., its Territories or Possessions, Puerto Rico or the Canal Zone, this Policy does not cover any liability of whatsoever nature directly or indirectly caused by or contributed to by or arising from ionising radiations or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel.

All other terms and conditions of this Policy shall remain unchanged.

This endorsement forms a part of the Policy to which attached, effective on the inception date of the Policy unless otherwise stated herein.

**BCS Insurance Company**
**2 Mid America Plaza, Suite 200**
**Oakbrook Terrace, IL 60181**
**(312) 803-7384**

# BREACH RESPONSE TEAM ENDORSEMENT

94.805 (06/17)

---

The following vendors have been approved to support “You” in the event of a “Security Breach”. “You” do not require “our” prior written consent to contact these vendors:

"Breach Response Counsel":

Baker & Hostetler LLP

24/7 Breach Response hotline - **1-866-288-1705**

"Breach Response Team":

Kroll

Data Breach Hotline - **1-877-300-6816**
**CyberResponse@kroll.com**

BCS Insurance Company
2 Mid America Plaza, Suite 200
Oakbrook Terrace, IL 60181
(312) 803-7384

# CONNECTICUT AMENDATORY ENDORSEMENT

94.801 CT (07/19)

This Endorsement, effective at 12:01 a.m. CST, on 03/18/2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

This endorsement modifies insurance provided under the following:

**CYBER AND PRIVACY LIABILITY POLICY**

The following changes are made to the policy:

I. The notice at the top of the first page of the Policy is replaced by the following:

**NOTICE: THIS POLICY IS LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST YOU DURING THE POLICY PERIOD (OR EXTENDED REPORTING PERIOD, IF APPLICABLE), AND LOSS FROM EVENTS THAT FIRST OCCUR AFTER THE RETROACTIVE DATE AND BEFORE THE END OF THE POLICY PERIOD THAT YOU FIRST LEARN OF DURING THE POLICY PERIOD AS REQUIRED HEREIN. CLAIMS EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION(S). TERMS THAT APPEAR IN "QUOTATIONS" HAVE SPECIAL MEANINGS. SEE THE DEFINITIONS FOR MORE INFORMATION. PLEASE READ THIS POLICY CAREFULLY.**

II. Section **I. COVERAGES**, paragraph **A. PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY)** is replaced by the following:

**A. PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY)**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" during the "Policy Period" or "Extended Reporting Period" arising out of a "Privacy Wrongful Act" occurring on or after the "Retroactive Date" and before the end of the "Policy Period", harming any third (3rd) party or "Employee".

III. Section **I. COVERAGES**, paragraph **A. PRIVACY LIABILITY (INCLUDING EMPLOYEE PRIVACY)** is replaced by the following:

**B. PRIVACY REGULATORY CLAIMS COVERAGE**

"We" shall pay on "Your" behalf "Regulatory Fines", "Consumer Redress Funds", "HIPPA Corrective Action Plan Costs, and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Regulatory Claim" first made against "You" during the "Policy Period" or "Extended Reporting Period" arising out of a "Privacy Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

IV. Section **I. COVERAGES**, paragraph **D. SECURITY LIABILITY** is replaced by the following:

**D. SECURITY LIABILITY**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" during the "Policy Period" or "Extended Reporting Period" arising out of a "Security Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

V. Section **I. COVERAGES**, paragraph **E. MULTIMEDIA LIABILITY** is replaced by the following:

**E. MULTIMEDIA LIABILITY**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" during the "Policy Period" or "Extended Reporting Period" arising out of a "Multimedia Wrongful Act" occurring after the "Retroactive Date" and before the end of the "Policy Period".

VI. Section **I. COVERAGES**, paragraph **H. PCI DSS ASSESSMENT** is replaced by the following:

**H. PCI DSS ASSESSMENT**

"We" shall pay on "Your" behalf "Damages" and "Claims Expenses" that "You" become legally obligated to pay in excess of the applicable retention resulting from a "Claim" first made against "You" during the "Policy Period" or "Extended Reporting Period" arising out of a "PCI DSS Wrongful Act" occurring on or after the "Retroactive Date" and before the end of the "Policy Period".

VII. Section **IV. EXCLUSIONS**, paragraph **H.** is replaced by the following:

H. Any strike or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; including all amounts, "Damages", or "Claim Expenses" 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 the above. However this exclusion does not apply to acts perpetuated electronically;

VIII. Section **V. DEFINITIONS** the definition of "Act of Terrorism" is deleted.

IX. Section **V. DEFINITIONS** the definition of **"Retroactive Date"** is replaced by the following:

"Retroactive Date" means the date specified in the Policy. Once established, the "Retroactive Date" may be advanced only with "Your" written consent.

X. The following is added to Section **V. DEFINITIONS**:

"Termination of Coverage" means, whether made by "Us" or by "You" at any time: (1) cancellation or non- renewal of this Policy; or (2) decrease in limits, reduction of coverage, increased deductible or self-insured retention, new exclusion, or any other change in coverage less favorable to "You".

XI. Section **VIII. EXTENDED REPORTING PERIOD** is replaced by the following:

**VIIIEXTENDED REPORTING PERIOD**

A. Basic "Extended Reporting Period": An basic "Extended Reporting Period" shall automatically be granted hereunder at no additional premium. The basic "Extended Reporting Period" shall start with "Termination of Coverage" and last for sixty (60) days. Such "Extended Reporting Period" shall cover "Claims" first made during such sixty (60) day "Extended Reporting Period" but only in respect of any act, error, or omission committed prior to the date of "Termination of Coverage", and subject to all other terms, conditions, and exclusions of this Policy. The limit of liability for the basic "Extended Reporting Period" shall be part of, and not in addition to, the "Policy Aggregate Limit.

B. "We" will advise "You" in writing of the basic "Extended Reporting Period" coverage and the availability of, the premium for, and the importance of purchasing the optional "Extended Reporting Period" coverage. "We" will send this advice no earlier than the date of notification of "Termination of Coverage" nor later than fifteen (15) days after the "Termination of Coverage".

C. Optional "Extended Reporting Period":

1. "You" shall have the right, upon payment in full and not proportionally or otherwise in part to have issued an endorsement providing a three (3) year optional "Extended Reporting Period". This optional "Extended Reporting Period" may be purchased at any time during the "Policy Period" but not later than thirty (30) days after the effective date of "Termination of Coverage".
2. Such optional "Extended Reporting Period" shall cover "Claims" made during this optional "Extended Reporting Period", but only in respect of any "Claim" arising out of any act, error, or omission committed prior to the date of "Termination of Coverage", and subject to all other terms, conditions, and exclusions of the Policy.
3. In the event of "Termination of Coverage", "You" shall have the greater of the following in which to submit written acceptance of the optional "Extended Reporting Period":
   a. Sixty (60) days from the effective date of "Termination of Coverage"; or
   b. Fifteen (15) days from the date of mailing or delivery of the advice required by paragraph B. above.
4. If the optional "Extended Reporting Period" is purchased, it will begin when the basic "Extended Reporting Period" coverage ends. "You" will have the option of either:
   a. Reinstating the "Policy Aggregate Limit" to one hundred percent (100%) for "Claims" first made during the optional "Extended Reporting Period"; or
   b. Including "Claims" first made during the optional "Extended Reporting Period" in the "Policy Aggregate Limit".
5. If, at the time "You" elect to purchase an optional "Extended Reporting Period", premium is due to "Us" for coverage under this Policy, any monies "We" receive from "You" as payment for the optional "Extended Reporting Period" shall be first applied to such premium owing for this Policy. The optional "Extended Reporting Period" will not take effect until the premium owing for this Policy is paid in full and unless the premium owing for the optional "Extended Reporting Period" coverage is paid promptly when due.

   The additional premium charged for the optional "Extended Reporting Period" shall be based upon rates in effect on the later of the date this Policy was issued or last renewed. "We" shall not charge a different premium for such coverage due to any change in "Our" rates, rating plans or rating rules subsequent to issuance or last renewal of this Policy. The additional premium shall be determined in accordance with the following schedule:

| Extended Reporting Period Length | Percent of Expiring Annual Premium Without Reinstatement of Policy Aggregate Limit | Percent of Expiring Annual Premium With Reinstatement of Policy Aggregate Limit |
|---|---|---|
| 3 years | 225% | 300% |

6. At the commencement of the optional "Extended Reporting Period", the entire premium shall be deemed fully earned, and in the event "You" terminate the optional "Extended Reporting Period" for whatever reason prior to its expiration, "We" will not be liable to return any premium paid for the optional "Extended Reporting Period".

D. All notices and premium payments with respect to the "Extended Reporting Period" shall be directed to "Us" through the entity named in the Policy.

XII. Section **IX. TERMS AND CONDITIONS**, paragraph **A. NOTICE OF CLAIM OR CIRCUMSTANCE THAT MIGHT LEAD TO A CLAIM**, item **4.** is replaced by the following:

4. Whenever coverage under this Policy would not be provided because of non-compliance of Section IX.A.1. relating to the giving of notice of "Claim" or "Loss" to "Us" with respect to which any other of "You" shall be in default solely because of the failure to give such notice or concealment of such failure by one or more of "You" who are responsible for the loss or damage otherwise insured hereunder, then "We" agree that such insurance as would otherwise be afforded under this Policy shall cover and be paid with respect to those of "You" who did not personally commit or personally participate in committing or remain silent despite being aware of such failure to give notice, provided that those of "You" entitled to the benefit of this provision under Section IX.A.1. have complied with such condition promptly after obtaining knowledge of the failure of any others of "You" to comply therewith, and any such "Claim" or "Loss" was reported during the "Policy Period" or "Extended Reporting Period", if applicable.

XIII. Section **IX. TERMS AND CONDITIONS**, paragraph **K. CANCELLATION AND NON-RENEWAL** is replaced by the following:

**K. CANCELLATION AND NON-RENEWAL**

1. This Policy may be cancelled by "You" at any time on request by sending a prior written notice to "Us" stating when thereafter the cancellation will be effective.
2. "We" may not cancel this Policy, except for nonpayment of premium. If "We" cancel this Policy for non-payment of premium, "We" will mail or deliver written notice to the all Named Insureds, including the actual reason for cancellation, at least ninety (90) days before the effective date of cancellation. However, "You" may continue this Policy and avoid the effect of the cancellation by payment in full at any time prior to the effective date of cancellation. Non-payment of any retention shall not be considered non-payment of premium for purposes of cancellation.
3. If this Policy is cancelled by "You", "We" shall refund the unearned premium computed pro-rata. If this Policy is cancelled by "Us", the refund of paid premium shall be computed pro-rata. Payment or tender of any unearned premium by "Us" shall not be a condition precedent to the effectiveness of such termination, but such payment shall be made as soon as practicable. No premium will be refunded where any "Claims" or circumstances have been notified under this Policy.
4. "We" may non-renew this Policy by mailing or delivering written notice, including the actual reason for non-renewal, to all Named Insureds at least ninety (90) days before the expiration date of this Policy. No notice is required if "You" fail to pay any advance premium required for renewal.

   If "We" fail to provide the Named Insureds with the required notice of non-renewal within the required time limit, "You" shall be entitled to a renewal of this Policy for a term of not less than one (1) year on the same terms as the expiring Policy, and the privilege of pro-rata cancellation at the lower of the current or previous year's rates if "You" exercise this option within ninety (90) days from the renewal or anniversary date.
5. "We" will mail or deliver all notices to all Named Insureds at the address shown in the Policy. If notice is mailed, it will be mailed by registered or certified mail or by mail evidenced by a United States Post Office certificate of mailing. Proof of mailing shall be sufficient proof of notice.

XIV. Section **IX. TERMS AND CONDITIONS**, paragraph **M. NAMED INSURED AUTHORIZATION**, item **1.** is deleted.

XV. Section **IX. TERMS AND CONDITIONS**, paragraph **P. CHOICE OF LAW** is replaced by the following:

**P. CHOICE OF LAW**

Any disputes involving this Policy shall be resolved applying the laws of the state of Connecticut.

All other terms and conditions of this Policy shall remain unchanged.

This endorsement forms a part of the Policy to which attached, effective on the inception date of the Policy unless otherwise stated herein.

**BCS Insurance Company**
**2 Mid America Plaza, Suite 200**
**Oakbrook Terrace, IL 60181**
**(312) 803-7384**

# Coverage for Certified Acts of Terrorism

## CYBER AND PRIVACY LIABILITY POLICY

94.551 (01/15)

This Endorsement, effective at 12:01 a.m. CST, on March 18, 2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

Issued by: BCS Insurance Company

In consideration of the additional premium payment of $198, the Exclusion under this Policy for acts of "Terrorism" that are certified by the Secretary of the Treasury as "Certified Acts of Terrorism" pursuant to the federal Terrorism Risk Insurance Act is hereby deleted, subject to the following provisions and restrictions:

**A.** With respect to any one or more "Certified Acts of Terrorism", "We" will not pay any amounts for which "We" are not responsible under the terms of the federal Terrorism Risk Insurance Act of 2002 (including subsequent action of Congress pursuant to the Act) due to the application of any clause which results in a cap on "Our" liability for payments for "Certified Acts of Terrorism" losses.

**B.** The terms and limitations of any "Terrorism" Exclusion, or the inapplicability or omission of a "Terrorism" Exclusion, do not serve to create coverage for any loss which would otherwise be excluded under this Policy, such as losses excluded under a Nuclear Incident Exclusion or Radioactive Contamination Exclusion.

All other terms and conditions of this Policy shall remain unchanged.

This endorsement forms a part of the Policy to which attached, effective on the inception date of the Policy unless otherwise stated herein.

**BCS Insurance Company**
**2 Mid America Plaza, Suite 200**
**Oakbrook Terrace, IL 60181**
**(312) 803-7384**

# Terrorism Exclusion Endorsement - Connecticut

## CYBER AND PRIVACY LIABILITY POLICY

94.554 CT (12/17)

This Endorsement, effective at 12:01 a.m. CST, on March 18, 2021 forms part of:

Policy No.: RPS-Q-50199854M/1

Issued to: City of Derby CT

Issued by: BCS Insurance Company

The following changes are made to the Policy:

I. The following is added to Section **IV. EXCLUSIONS**:

Any “Certified Act of Terrorism”.

II. The following are added to Section **V. DEFINITIONS:**

**"Certified Act of Terrorism"** means an act that is certified by the Secretary of the Treasury, in consultation with the Secretary of Homeland Security and the Attorney General of the United States, to be an act of terrorism pursuant to the federal Terrorism Risk Insurance Act. The criteria contained in the Terrorism Risk Insurance Act for a certified act of terrorism include the following:

a. The act resulted in insured losses in excess of $5 million in the aggregate, attributable to all types of insurance subject to the Terrorism Risk Insurance Act; and

b. The act is a violent act or an act that is dangerous to human life, property or infrastructure and is committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

All other terms and conditions of this Policy shall remain unchanged.

This endorsement forms a part of the Policy to which attached, effective on the inception date of the Policy unless otherwise stated herein.