Cyber Insurance in a
Connected World

- “Cyber is uncharted territory. It’s going to get worse, not better.”

- “We have a pretty good idea on how to properly assess the probabilities for earthquakes and hurricanes, but not with computer hacking threats.”

- “We don’t want to be a pioneer on this… I think anybody that tells you now they think they know in some actuarial way either what the general experience is like in the future, or what the worst case can be, is kidding themselves.”

Warren Buffet
Annual Shareholders Meeting
May 5th 2018

SCOPE OF COVERAGE SPECIMEN – CYBER INSURANCE CHECKLIST

POLICY FORM: Claims Made
Retro Date: Inception Date of Policy

	LIMIT	RETENTION
I. POLICY AGGREGATE LIMIT	**$1,000,000**	

A. Applicable to all sections except Incident Response Fund, which is its own separate aggregate.

II. THIRD PARTY LIABILITY – Data or Systems Related Loss (Damages and Legal defense expenses)	**$1,000,000**	**$2,500**

A. Cyber, Privacy and Network Security Liability

1. Breach of Protected Information (PII, HIPPA, etc.)
2. Breach of third party Confidential or Property Information:
   a) that is not available to or known by the general public or
   b) which the insured is legally responsible to maintain in confidence
3. includes both malicious (hacking, phishing, etc.) and accidental breaches
4. Transmissions of virus, malware, etc. from your system to other systems
5. Payment card liability (PCI/DSS) under a merchant Processing Agreement
6. Regulatory proceedings, fines and penalties (related to Cyber or Privacy laws)

B. Media Content Liability (libel, slander, copyright infringement, etc.)	**$1,000,000**	**$2,500**

1. Website content
2. Social media content

III. FIRST PARTY COVERAGE – Data or Systems Related Loss

A. Cyber Incident Response Fund – Via Chubb Response Team Panel **$1,000,000 $0**
-- Via Non-Panel Providers **$500,000 $2,500**

1. Response Team Expenses
   a) Cyber Incident Coach / Coordinator
   b) Cyber Forensics
   c) PR or Crisis Management Firm to protect/restore reputation
   d) Retention of a law firm for compliance with cyber laws and regulations (multiple states)
   e) Notification letters, credit monitoring, call center expenses
   d) Other expenses/services deemed reasonable and necessary

B. Digital Data Recovery Expenses **$1,000,000 $2,500**
(i.e. hacking, errors, phishing, etc.)

1. Malicious or Non-Malicious Data Loss Expense/Recovery
2. Reimbursement of Fraudulent telephone toll charges on your telephone system
3. Replacement of physical hardware or equipment damaged by cyber incident.

C. Business Interruption and Extra Expenses from: **$1,000,000 $2,500**
(After 8 hour waiting period)

1. network security failure or malicious acts
2. network extortion threats
3. Reputation Damage (Extended period of attrition)
4. Non- Malicious system failure
5. Contingent Business Interruption (i.e. "shared" provider systems)

D. Network Extortion Expense, in connection with threats to: **$1,000,000 $2,500**

1. Release protected information
2. Cause a network security failure
3. Corrupt, damage or encrypt digital data
4. Inhibit access to your computer system

IV. CYBER CRIME – MONEY RELATED LOSS (See descriptions attached)

1. Computer Fraud Loss	**$250,000**	**$2,500**
2. Funds Transfer Fraud Loss	**$250,000**	**$2,500**
3. Social Engineering/Deception Fraud Loss	**$250,000**	**$10,000**
4. Escrow or Third Party Funds Loss		
5. Default limit for #3 & #4 above, if the transfer is not authorized by an employee acting in supervisory capacity, or an owner/Control Group person.	**$50,000**	**$10,000**

V. OTHER CONSIDERATIONS

1. ABA Endorsement (attached to quote) – gives choice of counsel to insured
2. Incident Response limit is outside of policy aggregate limit
3. Chubb provides a published roster of pre-arranged network of incident Response Team and Resources, based in USA (see attached)
4. Directors, Officers and Employees are included as "Insureds"
5. Definitions include the cloud and mobile devices

VI. POLICY EXCLUSIONS (See policy for all)

1. Securities Law or ERISA
2. Anti-Trust or unfair trade
3. Breach of Contract, except PCI (Visa) or other contractual obligation to maintain confidentiality
4. Bodily Injury or Property Damage
5. Intellectual Property or Trade Secrets of the Insured
6. Insured vs insured
7. Internet infrastructure or power grid outage

CYBER "CRIME COVERAGE" – GENERAL INSURANCE DESCRIPTIONS

1) **Computer Fraud:**

The unlawful taking of money arising as **a consequence of unauthorized entry by a 3rd party into the insured's computer system**, which results in altered or fraudulent electronic payment instructions (i.e. ACH/Bill Pay) causing funds to be diverted into the account of the fraudster, all occurring without the knowledge or participation of the insured. (Often occurs as a consequence of *phishing scams*, hacking login credentials or finding weak portals of entry)

2) **Funds Transfer Fraud:**

Fraudulent **instructions to a financial institution issued by a third party imposter** (non-employee) who falsely purports to be the insured/account holder and who instructs the institution to transfer, pay or deliver funds from the insured's account, typically by wire transfer, all occurring without the knowledge or participation of the insured. (Often occurs as a consequence of hacking email accounts, *phishing scams* and/or other unauthorized release of legitimate wire transfer credentials)

3) Social Engineering / Deception Fraud:

An intentional misleading of an employee of the insured through misrepresentation, which results in the transfer of payment of money to a 3rd party imposter purporting to be an authorized Vendor, Client or Employee of the insured. (Often occurs as a consequence of hacking email systems and accounts and/or telephone contact from impersonators)

4) Third Party Funds / Escrow:

If third party or escrow funds are exposed, the policy language of the particular policy should be referenced for applicability of any coverage. The desired wording is as follows: "The insurer's liability under this policy will apply only to Money, Securities or Property owned by the insured **or for which the insured is legally liable, or held by the insured in any capacity whether or not** the insured is liable."

Chubb Cyber Enterprise Risk Management Policy Quotation

CHUBB

Contact Information

To: [redacted]

Phone: [redacted]

Producer:

Email Address:

From: [redacted]

Date:
05-24-2019

Issuing Company:
ACE American Insurance Company

Phone:

Email:

Account Information

Applicant Name:

Applicant Address:

Type of submission:	New Business
Line of Coverage:	Chubb Cyber Enterprise Risk Management Policy
Policy Form:	PF-48169 (10/16)
Policy Period:	06-13-2019 To 06-13-2020

Cover Letter

Dear [redacted]

I am pleased to offer the attached indication for [redacted]

Thank you for considering Chubb as your market of choice. We look forward to working with you. Should you have any questions, please do not hesitate to contact me.

Sincerely,
[redacted]

Chubb Cyber Enterprise Risk Management Policy — Option: 1

Maximum Single Limit of Insurance	**$1,000,000**	**Premium**	
Maximum Policy Aggregate Limit of Insurance	**$1,000,000**	**Surcharges/Assessments/Taxes**	**$0.00**
		Annual Quoted Premium	

Optional Extended Reporting Period: 12 months for 100% of last annual premium

First Party Insuring Agreements

Check if Included	Insuring Agreement	Limit of Insurance Each Incident/Aggregate	Retention/Waiting Period Each Incident	Cyber Incident Response Coach Retention
☒	Cyber Incident Response Fund	Sidecar		
	Cyber Incident Response Team	$1,000,000/$1,000,000	$2,500	$0
	Non-Panel Response Provider	$500,000/$500,000	$2,500	$2,500
☒	Business Interruption Loss and Extra Expense	$1,000,000/$1,000,000	$2,500/8 Hours	N/A
☒	Contingent Business Interruption Loss and Extra Expense			
	Unscheduled Providers	$1,000,000/$1,000,000	$2,500/8 Hours	N/A
	Scheduled Providers	N/A	N/A	N/A
☒	Digital Data Recovery	$1,000,000/$1,000,000	$2,500	N/A
☒	Network Extortion	$1,000,000/$1,000,000	$2,500	N/A

* Limits will automatically increase to the limits referenced in the Cyber Incident Response Fund Sidecar endorsement option if the Cyber Incident Response Team is used and subject to all terms of the endorsement. Please refer to the terms and conditions of the Cyber Incident Response Fund Sidecar endorsement.

Third Party Liability Insuring Agreements

Check if Included	Insuring Agreement	Limit of Insurance Each Claim/Aggregate	Retention Each Claim	Retroactive Date	Pending or Prior Proceedings Date
☒	Cyber Privacy, Network and Security Liability	$1,000,000/$1,000,000	$2,500	06-13-2019	06-13-2019
	Payment Card Loss	$100,000/$100,000	$2,500	06-13-2019	06-13-2019
	Regulatory Proceedings	$1,000,000/$1,000,000	$2,500	06-13-2019	06-13-2019
☒	Electronic, Social, and Printed Media Liability	$1,000,000/$1,000,000	$2,500	06-13-2019	06-13-2019

Cyber Crime Insuring Agreements

Check if Included	Insuring Agreement	Limit of Insurance Each Incident/Aggregate	Retention/Waiting Period Each Incident
☒	Computer Fraud	$250,000/$250,000	$2,500
☒	Funds Transfer Fraud	$250,000/$250,000	$2,500
☒	Social Engineering Fraud	$250,000/$250,000	$10,000

Other Notes about this option

Subjectivities

Chubb hereby indicates the coverage described below. However, any obligations the Insurer may have under this indication are conditioned upon each of the following conditions having first been met.

Please Note the Following for the Terrorism Risk Insurance Act:

Coverage for acts of terrorism is included in your policy. The portion of your annual premium that is attributable to coverage for acts of terrorism is $0, and does not include any charges for the portion of losses covered by the United States government under the Act.

The Following Notices will be added to the basic contract(s)

Title	Form Number
Chubb Producer Compensation Practices & Policies	ALL-20887a (03/16)
Policyholder Notice Cyber Services for Loss Mitigation	PF-48260 (10/16)
Policyholder Notice Cyber Services for Incident Response	PF-48259 (10/16)
US Foreign Account Tax Compliance Act ("FATCA")	ALL-42490b (07/16)
U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") Advisory Notice to Policyholders	PF-17914a (04/16)
Trade or Economic Sanctions Endorsement	PF-46422 (07/15)
Policyholder Disclosure Notice Of Terrorism Insurance Coverage	TR-19606d (01/15)
Cap On Losses From Certified Acts Of Terrorism	PF-45354 (01/15)
Disclosure Pursuant To Terrorism Risk Insurance Act	TRIA-11d (03/16)
Signatures	CC-1k11h (03/14)

The Following Endorsement(s) will added to the basic contract(s)

Title	Form Number
General Enhancement Endorsement - Cyber	PF-49468 (08/17)
American Bar Association Enhancement Endorsement for Law Firms	PF-49455 (08/17)
Cyber Crime Endorsement	PF-48257 (05/17)
Duty To Defend A Regulatory Proceeding	PF-49445 (08/17)
Non-Malicious Computer Act – System Failure – Business Interruption and Contingent Business Interruption - Sublimit	PF-48275 (08/17)
Hardware or Equipment Replacement Endorsement	PF-49492 (08/17)
Extended Period of Attrition Endorsement	PF-49494 (08/17)
Cyber Incident Response Fund Side-Car	PF-48258 (12/17)
Unincorporated Small Business Endorsement	PF-49487(08/17)
Communications Decency Exclusion	PF-49483(08/17)
Amendatory Endorsement – Alabama	PF-48306(10/16)

Conditions of this Indication

This indication will remain valid until 07-23-2019.

If between the date of this Indication and the Effective Date of the policy there is a significant adverse change in the condition of this Applicant, or an occurrence of an event, or other circumstances which could substantially change the underwriting evaluation of the Applicant, then, at the Insurer's option, this indication may be withdrawn by written notice thereof to Applicant. The Insurer also reserves the right to modify the final terms and conditions upon review of the completed application and any other information requested by the underwriter herein. If such material change in the risk is discovered after binding, the insurance coverage will be void ab initio ("from the beginning").

FOR POLICIES EFFECTIVE JULY 21, 2011 AND SUBSEQUENT, WE REQUIRE THE PRODUCER TO PROVIDE THE "HOME STATE" AS DEFINED IN THE NONADMITTED AND REINSURANCE REFORM ACT OF 2010 (NRRA) UPON THE BINDING OF THIS PLACEMENT. IF THE STATE SET FORTH IN THE ABOVE-REFERENCED INSURED ADDRESS IS THE HOME STATE OF THE INSURED, NO ACTION IS REQUIRED. HOWEVER, IF THE HOME STATE OF THE INSURED IS OTHER THAN THAT SET FORTH IN THE INSURED ADDRESS, YOU MUST NOTIFY US IN WRITING PRIOR TO THE BINDING OF THIS PLACEMENT.

Note: If the Insuring Company noted above is Chubb Custom Insurance Company, Westchester Surplus Lines Insurance Company or Illinois Union Insurance Company, then this insurance is issued pursuant to the state Surplus Lines laws that the insured is domiciled. Persons insured by Surplus Lines carriers do not have the protection of the above captioned state's Guaranty Act to the extent of any right of recovery for the obligation of an insolvent unlicensed insurer.

Any applicable taxes, surcharges or countersignature fees, etc., are in addition to the above indicated figures. Your office is responsible for making State Surplus Lines Filings and complying with all applicable laws.

Sincerely,

[redacted]

Chubb. Insured.℠

Additional Insured – Blanket Pursuant to a Contract – Cyber ERM

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy

It is agreed that the **Policy** is amended as follows:

Section II, Definitions, **Insured**, is amended by adding the following:

Insured also means any natural person or entity for whom an **Organization** is required by written contract or agreement to provide insurance coverage under this **Policy** (hereinafter "**Additional Insured**"), but only with respect to **Claims**:

a. arising out of any **Incident** committed after the **Organization** and the **Additional Insured** entered into such written contract or agreement;

b. for any **Incident** committed by, on behalf of, or at the direction of the **Organization**; and

c. subject to the lesser of the limits of insurance required by such written contract or agreement between the **Organization** and the **Additional Insured**, or the applicable Limits of Insurance of this **Policy**.

However, no natural person or entity shall be an **Additional Insured** with respect to any **Claim** arising solely out of such natural person's or entity's independent act, error, or omission. In the event of a disagreement between the **Named Insured** and the natural person or entity as to whether the **Claim** arises solely out of such natural person's or entity's independent act, error, or omission, it is agreed that the **Insurer** shall abide by the determination of the **Named Insured** on this issue, and such determination shall be made by the **Named Insured** within 20 days of the notification of the applicable **Claim**.

Section III, Exclusions, Subsection B, EXCLUSIONS APPLICABLE TO SPECIFIC INSURING AGREEMENTS, is amended by deleting paragraph 3. Insured v. Insured, and replacing it with the following:

Insured v. Insured

solely with respect to Insuring Agreements E and F, brought or maintained by, on behalf of, or in the right of any **Insured** other than an **Additional Insured** as defined in this endorsement. Provided, however, solely with respect to Insuring Agreement E, this exclusion shall not apply to that part of any **Claim** alleging employee-related invasion of privacy or employee–related wrongful infliction of emotional distress in the event such **Claim** arises out of the loss of **Protected Information** resulting from a **Cyber Incident**.

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

Cyber Insurance Policy Applications

(With Cyber Crime Extension)

CHUBB

ACE American Insurance Company
436 Walnut St.
Philadelphia, PA 19106

Chubb Cyber Enterprise Risk Management Policy

Cyber and Privacy Insurance

New Business Application

NOTICE

***NOTICE*: THE THIRD PARTY LIABILITY INSURING AGREEMENTS OF THIS POLICY PROVIDE CLAIMS-MADE COVERAGE, WHICH APPLIES ONLY TO CLAIMS FIRST MADE DURING THE POLICY PERIOD OR AN APPLICABLE EXTENDED REPORTING PERIOD FOR ANY INCIDENT TAKING PLACE AFTER THE RETROACTIVE DATE BUT BEFORE THE END OF THE POLICY PERIOD.**

AMOUNTS INCURRED AS CLAIMS EXPENSES UNDER THIS POLICY SHALL REDUCE AND MAY EXHAUST THE APPLICABLE LIMIT OF INSURANCE AND WILL BE APPLIED AGAINST ANY APPLICABLE RETENTION. IN NO EVENT WILL THE INSURER BE LIABLE FOR CLAIMS EXPENSES OR THE AMOUNT OF ANY JUDGMENT OR SETTLEMENT IN EXCESS OF THE APPLICABLE LIMIT OF INSURANCE. TERMS THAT ARE UNDERLINED IN THIS NOTICE PROVISION HAVE SPECIAL MEANING AND ARE DEFINED IN SECTION II, DEFINITIONS. READ THE ENTIRE POLICY CAREFULLY.

INSTRUCTIONS

Please respond to answers clearly. Underwriters will rely on all statements made in this **Application**. This form must be dated and signed.

1. Applicant Information

Desired Effective Date Mm/dd/yyyy	
Applicant Name Click here to enter text.	
Applicant Address (City, State, Zip) Click here to enter text.	
Please list all Subsidiaries for which coverage is desired: Click here to enter text.	
Applicant Type Choose an item.	**Ownership Structure** Choose an item.
Website Address Click here to enter text.	**Year Established** Click here to enter text.
Global Revenue (Prior Fiscal Year) Click here to enter text.	**% Domestic Revenue** Click here to enter text.
Global Revenue (Current Projected Fiscal Year) Click here to enter text.	**% Online Revenue** Click here to enter text.
Total Number of Employees Enter a number or choose an item.	

Number of Records Containing Protected Information:

What is the maximum total number of unique individual persons or organizations whose **Protected Information** could be compromised in a not-yet-discovered **Cyber Incident**, or will be stored or transmitted during the **Policy Period** on the Applicant's **Computer System** or any **Shared Computer System** combined that relate to the Applicant's business?

This should include **Protected Information** of employees, retirees, customers, partners and other third parties that the Applicant is responsible for securing, including **Protected Information** that is secured by third parties under contract with the Applicant. Multiple records or types of **Protected Information** relating to the same unique individual person or organization should be considered a single record.

Enter a number or choose an item

2. Nature of Operations

Class of Business

Describe nature of business operations, products or services in layperson terms.

Does the Applicant currently or will the Applicant potentially operate as any of the following?

- Accreditation Services Provider
- Adult Content Provider
- Credit Bureau
- Cryptocurrency Exchange
- Data Aggregator/Broker/Warehouse
- Direct Marketer
- Gambling Services Provider
- Manufacturer of Life Safety Products/Software
- Media Production Company
- Payment Processor
- Peer To Peer File Sharing
- Social Media
- Surveillance
- Third Party Claims Adminstrator

Or does the Applicant derive more than 50% of its revenue from technology products and services (e.g. software, electronics, telecom)?

☐Yes ☐ No

If Yes, please provide details:

Click here to enter text.

3. Current Loss Information

Within the past three years, has the Applicant had any actual or potential **Incidents** or **Claims** to which the **Policy** would apply; or is the Applicant aware of any fact, circumstance, or situation that could resonably be expected to give rise to an **Incident** or **Claim** to which the **Policy** would apply? ☐ Yes ☐ No

If Yes please provide details:

Click here to enter text.

4. Cyber and Media Controls

Which of the following IT security controls does the Applicant have in place?	
1) Antivirus and Firewalls (Windows 7 or higher qualifies)	☐ Yes ☐ No ☐ Unknown
2) Encryption of Sensitive Data	☐ Yes ☐ No ☐ Unknown
3) Encryption of Mobile Computing Devices	☐ Yes ☐ No ☐ Unknown
4) Critical Software Patching Procedures	☐ Yes ☐ No ☐ Unknown
5) Critical Data Backup and Recovery Procedures	☐ Yes ☐ No ☐ Unknown
6) Formal Cyber Incident Response Plan	☐ Yes ☐ No ☐ Unknown
Does the Applicant accept payment card (Credit/debit card) transactions?	☐ Yes ☐ No
If Yes, is the Applicant PCI compliant? (via assessment or self-attestation)	☐ Yes ☐ No ☐ Unknown
Does the Applicant deal with protected health information as defined by HIPAA?	☐ Yes ☐ No
If Yes, is Applicant compliant with HIPAA and the HITECH Act?	☐ Yes ☐ No ☐ Unknown
Does the Applicant have operations or customers in California, or any responsibilities under the California Confidentiality of Medical Information Act?	☐ Yes ☐ No ☐ Unknown
Has the Applicant obtained legal review of its use of trademarks, including domain names?	☐ Yes ☐ No ☐ Unknown

5. Current Coverage

Does the Applicant currently purchase Professional Liability or E&O insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	☐ Yes ☐ No
Does the Applicant currently purchase Cyber or Privacy Liability insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	☐ Yes ☐ No
Does the Applicant currently purchase Media Liability Insurance? **If Yes**, what is the Retro Date? Click here to enter a date.	☐ Yes ☐ No
Does the Applicant intend to purchase E&O and/or Media coverage on a separate and distinct policy? (e.g. with a separate set of limits, or with another carrier?)	☐ Yes ☐ No

6. Desired Coverage (Only Enter Information For Desired Coverages)

	Retention	Limit	Commentary
Cyber and Media Coverages	$	$	

Enter any further commentary about desired coverage options.
Click here to enter text.

FRAUD WARNING STATEMENTS

The Applicant's submission of this **Application** does not obligate the **Insurer** to issue, or the Applicant to purchase, a policy. The Applicant will be advised if the **Application** for coverage is accepted. The Applicant hereby authorizes the **Insurer** to make any inquiry in connection with this **Application.**

Notice to Arkansas, Minnesota, New Mexico and Ohio Applicants: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policy holder or claimant for the purpose of defrauding or attempting to defraud the policy holder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory agencies.

Notice to District of Columbia Applicants: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Kentucky Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

Notice to Louisiana and Rhode Island Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

Notice to Alabama and Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to Oklahoma Applicants: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

Notice to Oregon and Texas Applicants: Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

Notice to Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

MATERIAL CHANGE

If there is any material change in the answers to the questions in this **Application** before the **Policy** inception date, the Applicant must immediately notify the **Insurer** in writing, and any outstanding quotation may be modified or withdrawn.

DECLARATION AND SIGNATURE

For the purposes of this **Application**, the undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this **Application** and any attachments or information submitted with this **Application**, are true and complete. The undersigned agree that this **Application** and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued and shall be deemed to be attached to and shall form a part of any such policy. The **Insurer** will have relied upon this **Application**, its attachments, and such other information submitted therewith in issuing any policy.

The information requested in this **Application** is for underwriting purposes only and does not constitute notice to the **Insurer** under any policy of a Claim or potential Claim.

This **Application** must be signed by the risk manager or a senior officer of the **Named Insured**, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date	Signature	Title

SIGNATURE - FOR ARKANSAS, MISSOURI, NEW MEXICO, NORTH DAKOTA AND WYOMING APPLICANTS ONLY

PLEASE ACKNOWLEDGE AND SIGN THE FOLLOWING DISCLOSURE TO YOUR **APPLICATION** FOR INSURANCE:

I UNDERSTAND AND ACKNOWLEDGE THAT THE **POLICY** FOR WHICH I AM APPLYING CONTAINS A DEFENSE WITHIN LIMITS PROVISION WHICH MEANS THAT **CLAIMS EXPENSES** WILL REDUCE MY LIMITS OF INSURANCE AND MAY EXHAUST THEM COMPLETELY. SHOULD THAT OCCUR, I SHALL BE LIABLE FOR ANY FURTHER CLAIMS **EXPENSES** AND **DAMAGES**.

Applicant's Signature (Arkansas, Missouri, New Mexico, North Dakota & Wyoming Applicants, In Addition To **Application** Signature Above):

Signed: _____ (must be Officer of Applicant)

Print Name & Title: _____

Date (MM/DD/YY): _____

Email/Phone: _____

SIGNATURE - FOR KANSAS AND ALASKA APPLICANTS ONLY

ELECTRONIC DELIVERY SUPPLEMENT:

You are required by law to obtain consent from insureds prior to engaging in any electronic delivery of insurance policies and/or other supporting documents in connection with the **Policy**. You have the right to:

Select electronic delivery - check here _____

Reject electronic delivery – check here _____

Applicant's Signature (Kansas and Alaska Applicants, In Addition To **Application** Signature Above):

FOR FLORIDA APPLICANTS ONLY:

Agent Name: _____

Agent License ID Number: _____

FOR IOWA APPLICANTS ONLY:

Broker: _____

Address: _____

Cyber Crime (Only if applying for this coverage)	
Does the Applicant require that all outgoing payments or funds transfers be subject to segregations of duties between initiation and authorization, such that no one individual can control the entire process?	☐Yes ☐No/Unknown
Does the Applicant require that all outgoing payments or funds transfers be subject to dual authorization by at least one supervisor after being initiated by a third employee?	☐Yes ☐No
If not, is there a specific amount over which such dual authorization is required?	☐Yes ☐No If yes enter amount
Does the Applicant confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers, and contact information) by a direct call using only the contract number previously provided by the vendor/supplier before the request was received?	☐Yes ☐No/Unknown

Stand – Alone Crime Insurance Policy Applications

Chubb Group of Insurance Companies
15 Mountain View Rd.
Warren, NJ 07059

CHUBB

ForeFront Portfolio 3.0SM
Crime Coverage Section
Law Firm Application Supplement

BY COMPLETING THIS CRIME LAW FIRM APPLICATION SUPPLEMENT THE APPLICANT IS APPLYING FOR COVERAGE WITH FEDERAL INSURANCE COMPANY (THE "COMPANY")

NOTICE: READ THE ENTIRE CRIME LAW FIRM APPLICATION SUPPLEMENT CAREFULLY BEFORE SIGNING

CRIME LAW FIRM APPLICATION SUPPLEMENT INSTRUCTIONS

1. Whenever used in this Crime Law Firm Application Supplement, the term "Applicant" shall mean the firm and all subsidiaries, unless otherwise stated.
2. Please attach the following:
   (a) Most recent annual financial statement, audited if outside audits are performed;
   (b) Copy of the firm's internal audit plan; and
   (c) Copy of the firm's vendor management guidelines.
3. Include all requested underwriting information and attachments. Provide a complete response to all questions and attach additional pages if necessary.
4. This supplement should be submitted in conjunction with the ForeFront Portfolio 3.0SM Newline or Renewal Application, as appropriate.

I. NAME, ADDRESS AND CONTACT INFORMATION

1. Name of **Applicant**: _____
2. Address of **Applicant**: _____
   City: _____ State: _____ Zip Code: _____
3. **Applicant** Web Site(s): _____
4. Name and address (if different than above) of primary contact (Managing Partner or similar person authorized to receive notices and information regarding the proposed policy):
   Name: _____ Title: _____ Address: _____
   City: _____ State: _____ Zip Code: _____ Telephone: _____ e-Mail: _____

II. GENERAL RISK INFORMATION

1. Are there any subsidiaries with operations other than as a law firm (Escrow, Title Agent, Collections, Investment Advisor, or similar company)? ☐ Yes ☐ No

   If "Yes", please attach an explanation.
2. Please provide a breakdown of the **Applicant's** top five areas of practice, based on a percentage of total revenues at most recent fiscal year end:

   Please indicate month and year: _____ Month _____ Year

Area of Practice	Percentage of Revenues (%)	Dollar Value of Revenues

III. INTERNAL CONTROLS

1. **Banking Controls**

   (a) Does the **Applicant** use Positive Pay or Reverse Positive Pay for all of the firm's bank accounts? ☐ Yes ☐ No

   (b) Does the **Applicant**:

   (i) Use competitive bidding for all high value supplies and services? ☐ Yes ☐ No

   (ii) Maintain levels of authority for approval of purchases? ☐ Yes ☐ No

   If "Yes", please describe: _____

   (iii) Maintain consistent vendor management procedures between client chargeable and firm chargeable account payables?

2. **Computer and Funds Transfer Controls**

   (a) Does the **Applicant**:

   (i) Have a written policy regarding authority for setting up electronic funds transfers? ☐ Yes ☐ No

   If "Yes", please describe the policy: _____

   _____

   (ii) Require the processing bank to verify approval of all transfers with someone other than the requester of the transfer? ☐ Yes ☐ No

   (iii) Have software safeguards in place to prevent access to transfer software or online banking portals? ☐ Yes ☐ No

   If "Yes", does the software provide an active audit trail of user access and transaction history? ☐ Yes ☐ No

   (iv) Maintain active intrusion detection, anti-virus and spam filtering software on all systems? ☐ Yes ☐ No

   If "Yes", are potential computer threats, which have been identified by the protection software immediately quarantined, preventing the user from overriding the warning? ☐ Yes ☐ No

   (v) Provide training and education to all employees regarding "phishing"? ☐ Yes ☐ No

3. **Clients**

   (a) Please describe any services, other than providing legal advice, which the **Applicant** provides for clients (attach separate sheet if necessary): _____

   _____

   (b) Does the **Applicant** or any of its attorneys exercise discretion or control over any of its clients' funds, accounts or materials other than as a custodian for the **Applicant's** client trust accounts? ☐ Yes ☐ No

   If "Yes", please describe (attach separate sheet if necessary): _____

   (c) Does the **Applicant** or any of its attorneys ever render investment advice to the **Applicant's** clients or manage their investments? ☐ Yes ☐ No

   If "Yes", please describe (attach separate sheet if necessary): _____

   (d) Is there a procedure in place to verify new clients (credit checks, background checks and conflict checks) prior to initiating any financial transaction with them? ☐ Yes ☐ No

(e) Please complete the following information regarding the **Applicant's** client trust accounts.

Type of Account	# of Accounts	Maximum Value	Average Monthly Value
IOLTA Trust			
Common Client Trust (Non-IOLTA)			
Dedicated Probate/Estate Trust			
Dedicated Real Estate Client Trust			
Other Trust Accounts (describe)			

(f) Do the individuals that reconcile monthly client trust bank statements also handle deposits, have check signing authority or have access to check signing equipment (i.e. signature plates, stamps, online computer passwords)? ☐ Yes ☐ No

If "Yes", will the Applicant change the reconciliation process so that it is not done by the same individuals that handle deposits, sign checks or have access to check signing equipment? ☐ Yes ☐ No

(g) Is check signing limited to the trustee(s) of the funds? ☐ Yes ☐ No

If "No", who is authorized to sign client trust account checks? _____

Please describe the oversight process performed to guard against theft (attach separate sheet if necessary): _____

(h) Can checks be made payable to "Cash", "Bearer" or "Currency"? ☐ Yes ☐ No

(i) How often do clients receive an accounting of their trust account? _____

4. **Past Activities**

(a) Please attach a list all employee theft, forgery, computer fraud or other crime losses discovered by the **Applicant** in the last 5 years, itemizing each loss separately. Include date of loss, description and total amount of loss; or indicate ☐.

IV. MATERIAL CHANGE:

If there is any material change in the answers to the questions in this Crime Law Firm Application Supplement before the policy inception date, the **Applicant** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.

V. DECLARATIONS, FRAUD WARNINGS AND SIGNATURES:

The **Applicant's** submission of this Crime Law Firm Application Supplement does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the Crime Law Firm Application Supplement for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this Crime Law Firm Application Supplement.

The undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare that to the best of their knowledge and belief, after reasonable inquiry, the statements made in this Crime Law Firm Application Supplement and in any attachments or other documents submitted with this Crime Law Firm Application Supplement are true and complete. The undersigned agree that this Crime Law Firm Application Supplement and such attachments and other documents shall be the basis of the insurance policy should a policy providing the requested coverage be issued; that all such materials shall be deemed to be attached to and shall form a part of any such policy; and that the Company will have relied on all such materials in issuing any such policy.

The information requested in this Crime Law Firm Application Supplement is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.

Notice to Alabama and Maryland Applicants: Any person who knowingly and willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly and willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Arkansas, New Mexico and Ohio Applicants: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policy holder or claimant for the purpose of defrauding or attempting to defraud the policy holder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory agencies.

Notice to District of Columbia Applicants: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Kentucky Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

Notice to Louisiana and Rhode Island Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to Oklahoma Applicants: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

Notice to Oregon and Texas Applicants: Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

Notice to Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

SIGNATURE OF APPLICANT'S AUTHORIZED REPRESENTATIVE

Date	Signature*	Title
_____	_____	_____

*This Crime Law Firm Application Supplement must be signed by the managing general partner, president, or chief financial officer of the **Applicant** acting as the authorized representatives of the person(s) and entity(ies) proposed for this insurance.

Produced By:

Agent (Print & Sign): _____ _____

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

Submitted By:

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

CHUBB

Chubb
15 Mountain View Rd.
Warren, NJ 07059

ForeFront Portfolio 3.0℠
Social Engineering Fraud Supplemental Application

BY COMPLETING THIS APPLICATION YOU ARE APPLYING FOR COVERAGE WITH FEDERAL INSURANCE COMPANY (THE "COMPANY")

NOTICE: THE COVERAGE AFFORDED UNDER THIS COVERAGE SECTION DIFFERS IN SOME RESPECTS FROM THAT AFFORDED UNDER OTHER POLICIES. READ THE ENTIRE APPLICATION CAREFULLY BEFORE SIGNING.

APPLICATION INSTRUCTIONS:

1. Whenever used in this Application, the term "**Applicant**" shall mean the Parent Organization and all organizations applying for coverage.

2. Include all requested underwriting information and attachments. Provide a complete response to all questions and attach additional pages if necessary.

I. GENERAL INFORMATION:

1. Name of **Applicant**: _____

2. Address of **Applicant**: _____

   City: _____ State: _____ Zip Code: _____

3. **Applicant's** State of Incorporation: _____ and date established: _____

4. **Applicant** Web Site(s): _____

5. Limit Requested by **Applicant**: _____

II. SPECIFIC INFORMATION:

1. CUSTOMER AND CLIENT CONTROLS

Explain any "NO" answers, where indicated, at the END of this application.

1. Does the **Applicant** have a procedure in place to verify new customers or clients prior to initiating any financial transaction with them?

   If "Yes", check all that apply: ☐ Yes ☐ No

   a. D&B Report or other credit worthiness check? ☐ Yes ☐ No
   b. Bank account verification (name, address, contact info matching customer file)? ☐ Yes ☐ No
   c. Confirmation of physical address? ☐ Yes ☐ No
   d. Other (please describe) _____

2. Does the **Applicant** have custody or control over any funds or accounts of any of its clients, have access to clients' accounting, payroll, purchasing systems, or perform bill payment services, including but not limited to escrow or trust accounts? ☐ Yes ☐ No

   If "No", please skip to question 4.

   If "Yes", please describe by attachment to the application.

3. Does the **Applicant** accept funds transfer instructions from clients over the telephone, email, text message or similar method of communication? ☐ Yes ☐ No

   If "Yes", prior to complying with the instruction do you authenticate such instructions? (Check all methods that apply) ☐ Yes ☐ No

   a. Calling the customer at a predetermined number? ☐ Yes ☐ No
   b. Sending a text message to a predetermined number? ☐ Yes ☐ No
   c. Requiring receipt of a code known only to the customer to confirm identity? ☐ Yes ☐ No
   d. Some other method or combination of the above? ☐ Yes ☐ No

   (Please describe in an attachment to the Application).

4. Does the **Applicant** allow prepayment by customers or clients for products or services to be performed at a later date? If "Yes", please describe by attachment to the application. ☐ Yes ☐ No

5. Does the **Applicant** have a procedure to verify incoming checks have fully cleared the issuing financial institution prior to performing services, or wire transferring money? ☐ Yes ☐ No

3. VENDOR AND SUPPLIER CONTROLS

Explain any "NO" answers, except indicated otherwise, at the END of this application.

1. Does the **Applicant** confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers and contact information) by a direct call using only the contact number previously provided by the vendor/supplier before the request was received? ☐ Yes ☐ No

2. Does the **Applicant** send all confirmations of changes requested by the vendor/supplier to a person independent of the requestor of the change, with any changes being implemented only after the vendor/supplier has the opportunity to challenge them? ☐ Yes ☐ No

3. Does the **Applicant** require review of all changes to vendor/supplier records by a supervisor or next-level approver before any change to the record is processed? ☐ Yes ☐ No

4. Does the **Applicant** run exception reports, either automatic, or manually created, showing all changes to the standing data of vendors/suppliers? ☐ Yes ☐ No

   If "Yes", how often are the reports run, and by whom are they reviewed? _____

5. If "No" to any of the above questions, please describe the method by which vendor/supplier data is verified by the **Applicant**:

   _____

   _____

   _____

   _____

4. VOICE AND ELECTRONIC INITIATED TRANSFER CONTROLS

Explain any "NO" answers, except indicated otherwise, at the END of this application.

1. Does the **Applicant** maintain a pre-established list of employees authorized to transfer the **Applicant's** funds or initiate payments, when such request is from an internal company source (i.e. another employee, officer, subsidiary, location or business unit)? If yes, please attach a complete list, including titles and geographic locations. ☐ Yes ☐ No
2. Does the **Applicant** require that all outgoing payments or funds transfers be subject to segregation of duties between initiation and authorization, such that no one individual can control the entire process? ☐ Yes ☐ No
3. Does the **Applicant** require that outgoing payments or funds transfers be subject to dual *authorization* by at least one executive? ☐ Yes ☐ No

   If "No", is there a specific amount over which dual authorization is required?

   If so, what is this amount? $_____ (attach additional pages if necessary)
4. Does the **Applicant** allow authority for wire transfers to be delegated or verbally approved the time of a request? ☐ Yes ☐ No
5. Does the **Applicant** perform funds transfers to countries outside of the United States of America? ☐ Yes ☐ No

   If "Yes", which countries? _____
6. Does the **Applicant's** wire transfer system or accounting system maintain an active audit trail of authority for all funds transfers approved and released? ☐ Yes ☐ No
7. Does the **Applicant's** email server and/or internet service provider (ISP) use email authentication methods (such as Sender Policy Framework (SPF), Sender ID, DomainKeys Identified Mail (DKIM)) to detect spoofed email not originating from your domain? ☐ Yes ☐ No
8. Does the **Applicant's** email client perform address verification, matching "From" addresses displayed to end users with the email envelope's actual sender address, flagging, blocking or quarantining those that do not match as potentially spoofed email not originating from your domain? ☐ Yes ☐ No
9. Are finance employees that are responsible for wire transfer provided anti-fraud training, including but not limited to detection of social engineering, phishing and other scams? ☐ Yes ☐ No

   If "Yes", please describe: _____
10. Does the **Applicant** conduct penetration testing, simulated phishing attacks or other interactive intrusion testing of employees throughout the year? ☐ Yes ☐ No
11. Please describe any other means by which unauthorized payment requests made by vendors, clients or employees are screened for and detected by the **Applicant**.

    _____

    _____
12. Are international and domestic wire transfer procedures performed consistently across all business units? ☐ Yes ☐ No

    If "No", please explain any differences in an attachment to this application.

5. LOSS EXPERIENCE

List all employee theft, burglary, robbery, forgery, computer fraud or other crime losses discovered by the **Applicant** in the last five years, itemizing each loss separately (attach additional pages if necessary): ☐ *Check if none.*

Date of Loss	Description of Loss (Include controls that were circumvented, controls that were missing, and steps taken to remediate the causes of the loss)	Total Amount of Loss	Please indicate whether or not the loss was covered under another insurance policy and include the carrier's name	
			Covered: Yes or No?	Carrier's Name
			☐ Yes ☐ No	
			☐ Yes ☐ No	

6. PLEASE ATTACH THE FOLLOWING ADDITIONAL INFORMATION:

- An explanation of any answers requiring additional information as referenced in the application.
- A copy of the **Applicant's** wire transfer authority protocols and procedures.

III. NOTICES:

The **Applicant's** submission of this Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this Application.

Notice to Alabama and Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Arkansas, New Mexico and Ohio Applicants: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policy holder or claimant for the purpose of defrauding or attempting to defraud the policy holder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory agencies.

Notice to District of Columbia Applicants: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Kentucky Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

Notice to Louisiana and Rhode Island Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to Oklahoma Applicants: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

Notice to Oregon and Texas Applicants: Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

Notice to Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

IV. MATERIAL CHANGE:

If there is any material change in the answers to the questions in this Application before the policy inception date, the **Applicant** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.

V. DECLARATION AND SIGNATURE:

For the purposes of this Application, the undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this Application and any attachments or information submitted with this Application, are true and complete. The undersigned agree that this Application and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued and shall be deemed to be attached to and shall form a part of any such policy. The Company will have relied upon this Application, its attachments, and such other information submitted therewith in issuing any policy.

The information requested in this Application is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.

This Application must be signed by the risk manager or a senior officer of the Parent Organization, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date	Signature	Title
_____	_____	_____

Produced By:

Agent (Print & Sign): _____ _____

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

Submitted By:

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

What Have We Paid Lately

Cyber Claims Scenarios

CHUBB

Type of Claim	Details of Claim
Ransomware Attacks	• A professional services firm experienced a ransomware attack which encrypted several files on its servers. A ransom of approximately $10,000 was initially demanded. We were promptly notified of the event through our cyber incident response hotline and an incident response coach and a forensic firm that specialized in ransomware were retained from our cyber panel. After consulting with these experts, the Insured decided to pay the ransom. Upon payment of the ransom, the Insured was able to begin the decryption process. Following an investigation by the forensic firm, it was determined that no personally identifiable information was compromised as a result of the attack. As a result of the ransomware attack, the Insured incurred losses of approximately $100,000, which was comprised of $15,000 for the incident response coach, $75,000 for the forensic firm and $10,000 for the ransom payment.

Type of Claim	Details of Claim
Phishing Emails	• Employees of a midsize financial services company fell victim to a mass phishing attack by clicking on a link that enabled the bad actors to obtain system credentials which allowed them to access email accounts. Approximately 100 email accounts were compromised and the bad actors set a forwarding rule that sent new emails to an unauthorized webmail address. Many of the email accounts contained names and social security numbers of the Insured's clients. A cyber incident response coach and a forensics firm that frequently deals with these types of phishing scams were retained from our cyber panel. Utilizing specialized tools to analyze which email accounts were comprised, the forensics firm concluded that several million documents needed to be reviewed to determine the nature and scope of the affected population. Additionally, the bad actors were able to access the Insured's other systems to cause several fraudulent wire transfers to take place. It was eventually determined that 200,000 people needed to be notified and provided with two years of credit monitoring. Total first party losses were approximately $3.5M, broken down as follows: $2M for the forensics firm, $1M for the incident response coach and $500,000 credit monitoring and call center fees.
Vendor/Supply Chain	• A business associate of the Insured fell victim of a ransomware attack that encrypted many of its files. The business associate possessed medical records and personal health information of the Insured's customers and had to retain an incident response coach and forensic firm to remedy the ransomware attack on its system. While our Insured had previously utilized Chubb's pre-incident services to better prepare for a breach, the Insured still needed to consult with its own incident response coach from our cyber panel to determine what reporting obligations it had under HIPAA. The incident repsonse coach eventually determined that there was no exfiltration of personal health information from the business associate's system. As a result of the incident, the Insured incurred $20,000 in first party costs.
Unauthorized Access (Canada)	• Our Insured is a professional organization that has an online portal for its members to access data. The organization experienced a security incident and its service representatives noticed that in a number of instances, member registration information was incorrect and that there had been a scrambling of data. A incident response coach and a forensic service firm from our cyber panel were engaged and it was determined that unauthorized access occurred on one of its servers providing external web portal functionality. The forensic firm did not find any evidence that personally identifiable information was disclosed during the attack and the data returned from the Insured's database was non-sensitive. Chubb paid approximately $100,000 CAD in 1st party costs associated with this matter.

Contact Us

For more information on Chubb Cyber insurance solutions, please contact your local agent or broker, or visit www.chubb.com/us/cyber.

Chubb. Insured.℠

www.chubb.com/us/cyber
The content of this document is solely for informational purposes and is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb. Product highlights are summaries only; please see the actual policy for terms and conditions. Products and services may not be available in all locations, and remain subject to Chubb's underwriting criteria. Coverage is subject to the language of the policies as actually issued.
Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit www.chubb.com. Insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. Surplus lines insurance is sold only through licensed surplus lines producers.
©2018 Chubb 30-01-0061 (Ed. 1/18)

What Have We Paid Lately

Cyber Claims Scenarios

CHUBB

It's important to believe in how your insurance carrier responds to and manages your claim. We understand that when you purchase insurance, you are really buying peace of mind. Chubb's guiding claims principle is to handle claims with integrity, empathy, promptness, expertise and fairness.

Type of Claim	Details of Claim
SamSam Attack	A professional service firm was the target of a ransomware attack using the SamSam variety of malware. SamSam attacks have been on the rise as of late and the bad actors usually target open remote desktop ports. SamSam is different from other varieties of ransomware as it does not depend on a person opening an email attachment or going to a malicious website. In this instance, the Insured's backups were not sufficient and after consulting with an incident response coach and forensic vendor from our cyber panel, the decision was made to pay the ransom in Bitcoin.

Type of Claim	Details of Claim
Crypto Mining	A manufacturing company experienced a ransomware attack that resulted in the encryption of several of their files. After the Insured contacted Chubb through the 24/7 incident response hotline, we offered a consultation with an incident response coach and forensic experts from our cyber panel. As a result of these discussions, the Insured chose not to pay the ransom. However, once the forensic firm began working on remediating the ransomware attack, they discovered that the Insured was also the victim of crypto mining. The hacking group had installed software in the Insured's system that was mining Bitcoin. Crypto mining occurs when an unsuspecting party has coin mining (Bitcoin or other cryptocurrency) software installed into its system. As a result of crypto mining, the bad actor is able to secretly mine cryptocurrency at the expense of the Insured's system. This type of surreptitious mining operation leads to a drain on the Insured's processing power which extends to a degradation in service. In addition to the forensics firm and incident response coach, the Insured incurred credit monitoring and notification fees, as PII (personally identifiable information) was compromised in the attack.
DDoS Attack	A financial institution was the victim of a DDoS (distributed denial of service) attack over the course of a two month period, which periodically degraded the Insured's productivity. The DDoS attack crippled the Insured's system by overwhelming it with bogus internet traffic so that legitimate traffic could not get through to the Insured. The attack simultaneously originated from multiple sources so that it was difficult to stop. Working with the Chubb claims team, the Insured retained the services of an incident response coach and forensics firm to respond to this incident. This DDoS attack also caused the Insured to suffer a business interruption loss.
Loss of PHI	A healthcare organization was informed by law enforcement that its patients' information was found on the dark web. It is believed that criminals from outside the U.S. were able to exploit vulnerabilities in the Insured's system to access more than 200,000 patients' PHI (personal health information). Chubb assisted the Insured by retaining an incident response coach and a forensics firm from our cyber panel. Several governmental/ regulatory agencies were notified with the assistance of the coach. A call center was established and credit monitoring was offered to the affected patients.

Chubb Cyber Index℠

For more information on cyber claims, visit www.chubbcyberindex.com. This interactive platform showcases nearly two decades' worth of Chubb's proprietary commercial cyber claims data and is designed to provide insight into the real cyber threats facing organizations today, regardless of industry or size. View real time claims data right from your desktop or mobile device.

Contact Us

For more information on Chubb Cyber insurance solutions, contact your local agent or visit www.chubb.com/us/cyber.

Chubb. Insured.™

www.chubb.com/us/cyber
The content of this document is solely for informational purposes and is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb. Product highlights are summaries only; please see the actual policy for terms and conditions. Products and services may not be available in all locations, and remain subject to Chubb's underwriting criteria. Coverage is subject to the language of the policies as actually issued.
Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit www.chubb.com. Insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. Surplus lines insurance is sold only through licensed surplus lines producers.
©2018 Chubb 30-01-0061 (Ed. 6/18)

CHUBB®

What Have We Paid Lately

Cyber Claims Scenarios

It's important to believe in how your insurance carrier responds to and manages your claim. We understand that when you purchase insurance, you are really buying peace of mind. Chubb's guiding claims principle is to handle claims with integrity, empathy, promptness, expertise and fairness.

Risk	Industry	Business	Claim Difference
Biometric Cases	All	Commercial	Top-tier cyber defense counsel utilized
Physician Impersonation	Healthcare	Commercial	Expert claims investigatiom
BitPaymer Ransomware	Financial Institutions	Commercial	Technical expertise
Business Interruption	Retail	Commercial	Superior coverage

Claim Scenario Details

Biometric Cases

Companies that collect their employees' biometric information, including fingerprints, retinal scans, and facial recognition, are being sued in Illinois under the state's Biometric Information Privacy Act (BIPA). These lawsuits are usually brought as class actions and seek damages under BIPA. BIPA is an informed consent statute that protects a person's biometric information and creates a private right of action for individuals harmed by BIPA violations. Under the statute, plaintiffs can seek the greater of $1,000 or actual damages for each negligent violation, and the greater of $5,000 or actual damages for each intentional or reckless violation. A key BIPA case will be heard by the Illinois Supreme Court later this year and will have an impact on these matters.

Physician Impersonation

An Insured healthcare organization was notified by an outside firm that one of its doctors was being impersonated by an unlicensed physician posing as him. This imposter was able to review several medical files as part of a physician peer review process. Once the Insured became aware of the situation, it had to notify patients whose PHI (personal health information) was inappropriately exposed to this person. Several of the affected individuals have brought third party claims against the Insured for failing to safeguard their PHI.

Claim Scenario Details

BitPaymer is characterized by large ransom demands and in this instance, the demand was more than $500,000.

BitPaymer Ransomware

A financial service firm was the victim of a new strain of ransomware called BitPaymer. This type of ransomware encrypted the Insured's data, rendering it unusable. The bad actor also claimed to know that the Insured had the financial ability to pay the ransom. BitPaymer is characterized by large ransom demands (in the six-figures) and in this instance, the demand was more than $500,000. Additionally, BitPaymer is usually accompanied by the presence of a banking Trojan, which is a type of malware designed to steal a victim's financial information. In the present instance, the Insured's back-ups were also corrupted. Accordingly, after consulting with the Chubb cyber claims representative and incident response coach, the decision was made to pay the ransom, which was covered under the Chubb cyber policy.

After comparing the Insured's sales from the time of the attack to records of previous sales, Chubb paid a BI loss of more than $200,000.

Business Interruption

An Insured that sells retail goods was struck with a virulent strain of ransomware that encrypted its data, crippled its systems, and demanded $25,000 in Bitcoin. After consulting with their Chubb cyber claims representative, as well as an incident response coach and forensic expert from Chubb's cyber panel, the Insured decided to pay the ransom. The Insured received a decryption key that permitted access to the once-encrypted data. A forensic accountant was also retained from the Chubb panel and assisted in the calculation of the Insured's business interruption (BI) loss. After comparing the Insured's sales from the time of the attack to records of previous sales, Chubb paid a BI loss of more than $200,000.

Contact Us

For more information on Chubb Cyber insurance solutions, visit www.chubb.com/cyber.

Chubb. Insured.℠

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at www.chubb.com. In the United States, insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. Surplus lines insurance is sold only through licensed surplus lines producers. All products may not be available in all states. This communication contains product summaries only. This literature is descriptive only. Coverage is subject to the language of the policies as actually issued. Claims examples are based on actual US cases, composites of actual cases, or hypothetical situations. Resolution amounts are approximations of both actual and anticipated loss and defense costs. Facts may have been changed to protect confidentiality.

Form 30-01-0083 (Ed. 10/18)

CHUBB

Chubb
15 Mountain View Rd.
Warren, NJ 07059

ForeFront Portfolio 3.0[SM]
Social Engineering Fraud Supplemental Application

BY COMPLETING THIS APPLICATION YOU ARE APPLYING FOR COVERAGE WITH FEDERAL INSURANCE COMPANY (THE "COMPANY")

NOTICE: THE COVERAGE AFFORDED UNDER THIS COVERAGE SECTION DIFFERS IN SOME RESPECTS FROM THAT AFFORDED UNDER OTHER POLICIES. READ THE ENTIRE APPLICATION CAREFULLY BEFORE SIGNING.

APPLICATION INSTRUCTIONS:

1. Whenever used in this Application, the term "**Applicant**" shall mean the Parent Organization and all organizations applying for coverage.

2. Include all requested underwriting information and attachments. Provide a complete response to all questions and attach additional pages if necessary.

I. GENERAL INFORMATION:

1. Name of **Applicant**:
_____

2. Address of **Applicant**:_____
City: _____ State: _____ Zip Code: _____

3. **Applicant's** State of Incorporation: _____ and date established:_____

4. **Applicant** Web Site(s): _____

5. Limit Requested by **Applicant**: _____

II. SPECIFIC INFORMATION:

1. CUSTOMER AND CLIENT CONTROLS

Explain any "NO" answers, where indicated, at the END of this application.

1. Does the **Applicant** have a procedure in place to verify new customers or clients prior to initiating any financial transaction with them?

   If "Yes", check all that apply: ☐ Yes ☐ No

   a. D&B Report or other credit worthiness check? ☐ Yes ☐ No
   b. Bank account verification (name, address, contact info matching customer file)? ☐ Yes ☐ No
   c. Confirmation of physical address? ☐ Yes ☐ No
   d. Other (please describe)_____

2. Does the **Applicant** have custody or control over any funds or accounts of any of its clients, have access to clients' accounting, payroll, purchasing systems, or perform bill payment services, including but not limited to escrow or trust accounts? ☐ Yes ☐ No

   If "No", please skip to question 4.

   If "Yes", please describe by attachment to the application.

3. Does the **Applicant** accept funds transfer instructions from clients over the telephone, email, text message or similar method of communication? ☐ Yes ☐ No

   If "Yes", prior to complying with the instruction do you authenticate such instructions? (Check all methods that apply) ☐ Yes ☐ No

   a. Calling the customer at a predetermined number? ☐ Yes ☐ No
   b. Sending a text message to a predetermined number? ☐ Yes ☐ No
   c. Requiring receipt of a code known only to the customer to confirm identity? ☐ Yes ☐ No
   d. Some other method or combination of the above? ☐ Yes ☐ No

   (Please describe in an attachment to the Application).

4. Does the **Applicant** allow prepayment by customers or clients for products or services to be performed at a later date? If "Yes", please describe by attachment to the application. ☐ Yes ☐ No

5. Does the **Applicant** have a procedure to verify incoming checks have fully cleared the issuing financial institution prior to performing services, or wire transferring money? ☐ Yes ☐ No

3. VENDOR AND SUPPLIER CONTROLS

Explain any "NO" answers, except indicated otherwise, at the END of this application.

1. Does the **Applicant** confirm all changes to vendor/supplier details (including routing numbers, account numbers, telephone numbers and contact information) by a direct call using only the contact number previously provided by the vendor/supplier before the request was received? ☐ Yes ☐ No

2. Does the **Applicant** send all confirmations of changes requested by the vendor/supplier to a person independent of the requestor of the change, with any changes being implemented only after the vendor/supplier has the opportunity to challenge them? ☐ Yes ☐ No

3. Does the **Applicant** require review of all changes to vendor/supplier records by a supervisor or next-level approver before any change to the record is processed? ☐ Yes ☐ No

4. Does the **Applicant** run exception reports, either automatic, or manually created, showing all changes to the standing data of vendors/suppliers? ☐ Yes ☐ No

   If "Yes", how often are the reports run, and by whom are they reviewed? _____

5. If "No" to any of the above questions, please describe the method by which vendor/supplier data is verified by the **Applicant**:

   _____

   _____

   _____

   _____

4. VOICE AND ELECTRONIC INITIATED TRANSFER CONTROLS

Explain any "NO" answers, except indicated otherwise, at the END of this application.

1. Does the **Applicant** maintain a pre-established list of employees authorized to transfer the **Applicant's** funds or initiate payments, when such request is from an internal company source (i.e. another employee, officer, subsidiary, location or business unit)? If yes, please attach a complete list, including titles and geographic locations. ☐ Yes ☐ No
2. Does the **Applicant** require that all outgoing payments or funds transfers be subject to segregation of duties between initiation and authorization, such that no one individual can control the entire process? ☐ Yes ☐ No
3. Does the **Applicant** require that outgoing payments or funds transfers be subject to dual *authorization* by at least one executive? ☐ Yes ☐ No

   If "No", is there a specific amount over which dual authorization is required?

   If so, what is this amount? $_____ (attach additional pages if necessary)
4. Does the **Applicant** allow authority for wire transfers to be delegated or verbally approved the time of a request? ☐ Yes ☐ No
5. Does the **Applicant** perform funds transfers to countries outside of the United States of America? ☐ Yes ☐ No

   If "Yes", which countries? _____
6. Does the **Applicant's** wire transfer system or accounting system maintain an active audit trail of authority for all funds transfers approved and released? ☐ Yes ☐ No
7. Does the **Applicant's** email server and/or internet service provider (ISP) use email authentication methods (such as Sender Policy Framework (SPF), Sender ID, DomainKeys Identified Mail (DKIM)) to detect spoofed email not originating from your domain? ☐ Yes ☐ No
8. Does the **Applicant's** email client perform address verification, matching "From" addresses displayed to end users with the email envelope's actual sender address, flagging, blocking or quarantining those that do not match as potentially spoofed email not originating from your domain? ☐ Yes ☐ No
9. Are finance employees that are responsible for wire transfer provided anti-fraud training, including but not limited to detection of social engineering, phishing and other scams? ☐ Yes ☐ No

   If "Yes", please describe: _____
10. Does the **Applicant** conduct penetration testing, simulated phishing attacks or other interactive intrusion testing of employees throughout the year? ☐ Yes ☐ No
11. Please describe any other means by which unauthorized payment requests made by vendors, clients or employees are screened for and detected by the **Applicant**.

    _____

    _____
12. Are international and domestic wire transfer procedures performed consistently across all business units? ☐ Yes ☐ No

    If "No", please explain any differences in an attachment to this application.

5. LOSS EXPERIENCE

List all employee theft, burglary, robbery, forgery, computer fraud or other crime losses discovered by the **Applicant** in the last five years, itemizing each loss separately (attach additional pages if necessary): ☐ *Check if none.*

Date of Loss	Description of Loss (Include controls that were circumvented, controls that were missing, and steps taken to remediate the causes of the loss)	Total Amount of Loss	Please indicate whether or not the loss was covered under another insurance policy and include the carrier's name	
			Covered: Yes or No?	Carrier's Name
			☐ Yes ☐ No	
			☐ Yes ☐ No	

6. PLEASE ATTACH THE FOLLOWING ADDITIONAL INFORMATION:

- An explanation of any answers requiring additional information as referenced in the application.
- A copy of the **Applicant's** wire transfer authority protocols and procedures.

III. NOTICES:

The **Applicant's** submission of this Application does not obligate the Company to issue, or the **Applicant** to purchase, a policy. The **Applicant** will be advised if the Application for coverage is accepted. The **Applicant** hereby authorizes the Company to make any inquiry in connection with this Application.

Notice to Alabama and Maryland Applicants: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Arkansas, New Mexico and Ohio Applicants: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false, fraudulent or deceptive statement is, or may be found to be, guilty of insurance fraud, which is a crime, and may be subject to civil fines and criminal penalties.

Notice to Colorado Applicants: It is unlawful to knowingly provide false, incomplete or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policy holder or claimant for the purpose of defrauding or attempting to defraud the policy holder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory agencies.

Notice to District of Columbia Applicants: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

Notice to Florida Applicants: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

Notice to Kentucky Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

Notice to Louisiana and Rhode Island Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

Notice to Maine, Tennessee, Virginia and Washington Applicants: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

Notice to New Jersey Applicants: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

Notice to Oklahoma Applicants: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

Notice to Oregon and Texas Applicants: Any person who makes an intentional misstatement that is material to the risk may be found guilty of insurance fraud by a court of law.

Notice to Pennsylvania Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

Notice to Puerto Rico Applicants: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand (5,000) dollars and not more than ten thousand (10,000) dollars, or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances are present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

IV. MATERIAL CHANGE:

If there is any material change in the answers to the questions in this Application before the policy inception date, the **Applicant** must immediately notify the Company in writing, and any outstanding quotation may be modified or withdrawn.

V. DECLARATION AND SIGNATURE:

For the purposes of this Application, the undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance declare to the best of their knowledge and belief, after reasonable inquiry, the statements made in this Application and any attachments or information submitted with this Application, are true and complete. The undersigned agree that this Application and its attachments shall be the basis of a contract should a policy providing the requested coverage be issued and shall be deemed to be attached to and shall form a part of any such policy. The Company will have relied upon this Application, its attachments, and such other information submitted therewith in issuing any policy.

The information requested in this Application is for underwriting purposes only and does not constitute notice to the Company under any policy of a Claim or potential Claim.

This Application must be signed by the risk manager or a senior officer of the Parent Organization, acting as the authorized representative of the person(s) and entity(ies) proposed for this insurance.

Date	Signature	Title
_____	_____	_____

Produced By:

Agent (Print & Sign): _____ _____

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

Submitted By:

Agency: _____

Agency Taxpayer ID or SS No.: _____ Agent License No.: _____

Address: _____

City: _____ State: _____ Zip: _____

Specimen Policy Form

Cyber, with Cyber Crime Extension

In consideration of the payment of the premium, in reliance upon the **Application**, and subject to the Declarations and the terms and conditions of this **Policy**, the **Insureds** and the **Insurer** agree as follows:

I. INSURING AGREEMENTS

Coverage is afforded pursuant to those Insuring Agreements purchased, as shown in Item 4 of the Declarations.

FIRST PARTY INSURING AGREEMENTS

A. *CYBER INCIDENT RESPONSE FUND*

The **Insurer** will pay **Cyber Incident Response Expenses** incurred by an **Insured** in response to a **Cyber Incident** first discovered by any **Control Group Member** during the **Policy Period**.

B. *BUSINESS INTERRUPTION AND EXTRA EXPENSES*

The **Insurer** will pay:

1. the **Business Interruption Loss** and **Extra Expenses** incurred by an **Insured** during the **Period of Restoration** resulting directly from a **Cyber Incident** which first occurs during the **Policy Period**; and
2. the **Contingent Business Interruption Loss** and **Extra Expenses** incurred by an **Insured** during the **Period of Restoration** resulting directly from a **Cyber Incident** which first occurs during the **Policy Period**.

C. *DIGITAL DATA RECOVERY*

The **Insurer** will pay the **Digital Data Recovery Costs** incurred by an **Insured** resulting directly from a **Cyber Incident** first discovered by any **Control Group Member** during the **Policy Period**.

D. *NETWORK EXTORTION*

The **Insurer** will reimburse **Extortion Expenses** incurred by an **Insured** in response to a **Cyber Incident** first discovered by any **Control Group Member** during the **Policy Period**.

THIRD PARTY LIABILITY INSURING AGREEMENTS

E. *CYBER, PRIVACY AND NETWORK SECURITY LIABILITY*

The **Insurer** will pay **Damages** and **Claim Expenses** by reason of a **Claim** first made against an **Insured** during the **Policy Period** for a **Cyber Incident** which first occurs on or after the **Retroactive Date** and prior to the end of the **Policy Period**.

F. *ELECTRONIC, SOCIAL AND PRINTED MEDIA LIABILITY*

The **Insurer** will pay **Damages** and **Claim Expenses** by reason of a **Claim** first made against an **Insured** during the **Policy Period** for a **Media Incident** which first occurs on or after the **Retroactive Date** and prior to the end of the **Policy Period**.

II. DEFINITIONS

When used in this **Policy**:

Act of Cyber-Terrorism means: (i) any act, including force or violence, or the threat thereof, expressly directed against a **Computer System** operated by an **Insured,** by an individual or any group of individuals, whether acting alone, on behalf of or in connection with any entity or government to damage, destroy or access a **Computer System** without authorization; or, (ii) a targeted denial of service attack or transmittal of corrupting or harmful software code at or into the **Insured's Computer System** for social, ideological, religious, economic or political reasons, including intimidating or coercing a government, a civilian population or disrupting any segment of an economy.

Application means all applications, including any attachments thereto, and all other information and materials submitted by or on behalf of the **Insureds** to the **Insurer** in connection with the **Insurer** underwriting this **Policy** or any policy of which this **Policy** is a direct renewal or replacement. All such applications, assessments, attachments, information and materials are deemed attached to and incorporated into this **Policy**.

Bodily Injury means injury to the body, sickness, disease, or death. **Bodily Injury** also means mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock, whether or not resulting from injury to the body, sickness, disease or death of any person.

Business Interruption Loss means:

1. the **Insured's** continuing normal operating and payroll expenses; and
2. the **Insured's** net profit before income taxes that would have been earned had no **Interruption in Service** of the **Insured's Computer System** occurred.

Claim means any:

1. written demand against any **Insured** for monetary damages or non-monetary or injunctive relief;
2. civil proceeding against any **Insured** seeking monetary damages or non-monetary or injunctive relief, commenced by the service of a complaint or similar pleading;
3. arbitration or mediation proceeding against any **Insured** seeking monetary damages or non-monetary or injunctive relief, commenced by the receipt of a written demand, or service of a complaint or similar pleading;
4. criminal proceeding against an **Insured** commenced by: (a) an arrest, or (b) a return of an indictment, information or similar document;
5. written request directed at an **Insured** to toll or waive a statute of limitations applicable to a **Claim** referenced in paragraphs 1-4 immediately above; or
6. **Regulatory Proceeding**,

including, where applicable, any appeal therefrom.

Claims Expenses means the reasonable and necessary:

1. attorneys' fees, mediation costs, arbitration expenses, expert witness fees and other fees and costs incurred by the **Insurer**, or by an **Insured** with the **Insurer's** prior written consent, in the investigation and defense of a **Claim**; and
2. premiums for any appeal bond, attachment bond or similar bond, although the **Insurer** shall have no obligation to apply for or furnish such bond.

Claims Expenses shall not include wages, salaries or other compensation of directors, officers, similar executives, or employees of the **Insurer** or any **Insured**.

Computer System means computer hardware, software, **Telephone System**, firmware, and the data stored thereon, as well as associated input and output devices, data storage devices, networking equipment and storage area network or other electronic data backup facilities.

Consumer Redress Fund means a sum of money which an **Insured** is legally obligated to deposit in a fund as equitable relief for the payment of consumer claims due to an adverse judgment or settlement of a **Regulatory Proceeding**. **Consumer Redress Fund** shall not include any amounts paid which constitute taxes, fines, penalties, injunctive relief or sanctions.

Contingent Business Interruption Loss means:

1. the **Insured's** continuing normal operating and payroll expenses; and
2. the **Insured's** net profit before income taxes that would have been earned had no **Interruption in Service** of a **Shared Computer System** occurred.

Control Group Member means, as applicable, an **Organization's** Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer, Chief Technology Officer, General Counsel, Risk Manager, or the organizational or functional equivalent of such positions.

Costs means:

1. **Cyber Incident Response Expenses**;
2. **Business Interruption Loss**;
3. **Contingent Business Interruption Loss**;
4. **Extra Expenses**;
5. **Digital Data Recovery Costs**; or
6. **Extortion Expenses**.

Cyber Incident means:

1. with respect to Insuring Agreement A, Cyber Incident Response Fund,
   a. any actual or reasonably suspected **Network Security Failure**;
   b. any actual or reasonably suspected failure by an **Insured**, or any independent contractor for whom or for which an **Insured** is legally responsible, to properly handle, manage, store, destroy, protect, use or otherwise control **Protected Information**;
   c. any unintentional violation by an **Insured** of any **Privacy or Cyber Law**, including the unintentional wrongful collection of **Protected Information** by an **Insured**;
   d. any reasonably suspected **Interruption in Service**, provided a Limit of Insurance is shown in the Declarations applicable to Insuring Agreement B, Business Interruption And Extra Expenses; or
   e. any reasonably suspected **Network Extortion Threat**, provided a Limit of Insurance is shown in the Declarations applicable to Insuring Agreement D, Network Extortion;
2. with respect to Insuring Agreement B, Business Interruption And Extra Expenses, an actual **Interruption in Service**;
3. with respect to Insuring Agreement C, Digital Data Recovery, an actual **Network Security Failure** resulting in **Digital Data Recovery Costs**;
4. with respect to Insuring Agreement D, Network Extortion, an actual **Network Extortion Threat**; or
5. with respect to Insuring Agreement E, Cyber, Privacy And Network Security Liability, any error, misstatement, misleading statement, act, omission, neglect, breach of duty or other offense actually or allegedly committed or attempted by any **Insured** in their capacity as such, resulting in or based upon a **Cyber Incident** as referenced in paragraphs 1 – 4 immediately above.

Cyber Incident Response Coach means the law firm within the **Cyber Incident Response Team**, designated for consultative and pre-litigation legal services provided to an **Insured**.

Cyber Incident Response Expenses means those reasonable and necessary expenses paid or incurred by an **Insured** as a result of a **Cyber Incident**. Such expenses are as follows:

1. retaining the services of the **Cyber Incident Response Coach**;
2. retaining the services of a third party computer forensics firm to determine the cause and scope of a **Cyber Incident**;
3. retaining the services of a public relations or crisis communications firm for the purpose of protecting or restoring the reputation of, or mitigating financial harm to, an **Insured**;
4. retaining the services of a law firm to determine the **Insured's** rights under the indemnification provisions of a written agreement between the **Insured** and any other person or entity with respect to a **Cyber Incident** otherwise covered under Insuring Agreements A - E of this **Policy**;
5. expenses required to comply with **Privacy or Cyber Laws**, including:
   a. retaining the services of a law firm to determine the applicability of and actions necessary to comply with **Privacy or Cyber Laws**;

b. drafting notification letters, and to report and communicate as required with any regulatory, administrative or supervisory authority;

c. retaining call center and other related services for notification as required by law; or

d. providing credit monitoring, credit freezing or credit thawing.

For purposes of this paragraph 5, compliance with **Privacy or Cyber Laws** shall follow the law of the applicable jurisdiction that most favors coverage for such expenses;

6. expenses not required to comply with **Privacy or Cyber Laws**, and with the **Insurer's** prior consent, for:

   a. notifying a natural person whose **Protected Information** has been wrongfully disclosed or otherwise compromised, including retaining a notification service or the services of a call center;

   b. providing credit monitoring, credit freezing, credit thawing, healthcare record monitoring (where available), social media monitoring, password management service, or fraud alert services for those natural persons who accept an offer made by or on behalf of the **Insured** for, and receive, such services;

   c. retaining the services of a licensed investigator or credit specialist to provide fraud consultation to the natural persons whose **Protected Information** has been wrongfully disclosed or otherwise compromised;

   d. retaining the services of third party identity restoration service to natural persons identified by a licensed investigator as victims of identity theft directly resulting from a **Cyber Incident** otherwise covered under Insuring Agreements A or E;

   e. paying any reasonable amount to an informant for information not otherwise available which leads to the arrest and conviction of a natural person or an entity responsible for a **Cyber Incident**; or

   f. other services that are deemed reasonable and necessary by the **Insurer**.

Cyber Incident Response Expenses shall not include:

i. costs or expenses incurred to update or improve privacy or network security controls, policies or procedures, or compliance with **Privacy or Cyber Laws**, to a level beyond that which existed prior to the applicable **Cyber Incident**;

ii. taxes, fines, penalties, amounts for injunctive relief, or sanctions;

iii. the **Insured's** money or any money in the **Insured's** care, custody, or control; or

iv. wages, salaries, and other compensation of directors, officers, similar executives, or employees of an **Organization**, or internal operating costs, expenses, or fees of any **Organization**.

Cyber Incident Response Team means **Pre-Approved Service Providers** who provide services as defined in **Cyber Incident Response Expenses**.

Damages means compensatory damages, any award of prejudgment or post-judgment interest, **Payment Card Loss**, **Consumer Redress Fund**, settlements, and amounts which an **Insured** becomes legally obligated to pay on account of any **Claim**. **Damages** shall not include:

1. any amount for which an **Insured** is not financially liable or legally obligated to pay;

2. taxes, fines, penalties or sanctions imposed against an **Insured**, except for **Payment Card Loss** or **Regulatory Fines** otherwise covered under Insuring Agreement E;

3. matters uninsurable under the laws pursuant to which this **Policy** is construed;

4. punitive or exemplary damages, or the multiple portion of any multiplied damage award, except to the extent that such punitive or exemplary damages, or multiplied portion of any multiplied damage award, are insurable under the applicable laws of any jurisdiction which most favors coverage for such damages and which has a substantial relationship to the **Insured**, **Insurer**, this **Policy**, or the **Claim** giving rise to such damages;

5. the cost to an **Insured** to comply with any injunctive, remedial, preventative, or other non-monetary or declaratory relief, including specific performance, or any agreement to provide such relief;

6. consideration owed or paid by or to an **Insured**, including any royalties, restitution, reduction, disgorgement or return of any payment, charges, or fees; or costs to correct or re-perform services, or for the reprint, recall, or removal of **Media Content**;
7. liquidated damages pursuant to a contract, to the extent such amount exceeds the amount which the **Insured** would have been liable in the absence of such contract; or
8. penalties against an **Insured** of any nature, however denominated, arising by contract, except for **Payment Card Loss** otherwise covered under Insuring Agreement E.

Digital Data means software or other information in electronic form which is stored on an **Insured's Computer System** or **Shared Computer System**. **Digital Data** shall include the capacity of an **Insured's Computer System** or **Shared Computer System** to store information, process information, and transmit information over the Internet. **Digital Data** shall not include or be considered tangible property.

Digital Data Recovery Costs means:

1. the reasonable and necessary costs incurred by an **Insured** to replace, restore, recreate, re-collect or recover **Digital Data** from written records or from partially or fully matching electronic records due to their corruption, theft, or destruction, caused by a **Network Security Failure**, including disaster recovery or computer forensic investigation efforts. However, in the event that it is determined that the **Digital Data** cannot be replaced, restored, recreated, re-collected, or recovered, **Digital Data Recovery Costs** shall be limited to the reasonable and necessary costs incurred to reach such determination; or
2. **Telephone Fraud Financial Loss**,

including reasonable and necessary expenses incurred to mitigate or reduce any costs or loss in paragraphs 1 and 2 immediately above. **Digital Data Recovery Costs** shall not include:

a. costs or expenses incurred to update, replace, restore, recreate or improve **Digital Data** to a level beyond that which existed prior to the applicable **Cyber Incident**;
b. costs or expenses incurred to identify or remediate software program errors or vulnerabilities, or costs to update, replace, restore, upgrade, maintain, or improve a **Computer System**;
c. costs incurred to research and develop **Digital Data**, including **Trade Secrets**;
d. the economic or market value of **Digital Data**, including **Trade Secrets**; or
e. any other consequential loss or damages.

Extended Reporting Period means the period of time shown in Item 7B of the Declarations, subject to Section V, Extended Reporting Period.

Extortion Expenses means reasonable and necessary expenses incurred by an **Insured** resulting directly from a **Network Extortion Threat**, including money, cryptocurrencies (including Bitcoin), or other consideration surrendered as payment by an **Insured** to a natural person or group believed to be responsible for a **Network Extortion Threat**. **Extortion Expenses** shall also include reasonable and necessary expenses incurred to mitigate or reduce any of the forgoing expenses.

Extra Expenses means the reasonable and necessary:

1. expenses incurred by an **Insured** to the extent such expenses mitigate, reduce, or avoid an **Interruption in Service**, provided they are in excess of expenses that an **Insured** would have incurred had there been no **Interruption in Service**;
2. expenses incurred by an **Insured** to the extent such expenses reduce the **Period of Restoration**;
3. with the **Insurer's** prior consent, costs incurred by an **Insured** to retain the services of a third party forensic accounting firm to determine the amount of **Business Interruption Loss** or **Contingent Business Interruption Loss**.

   Extra Expenses shall not include:

   a. costs or expenses incurred to prevent a loss or correct any deficiencies or problems with an **Insured's Computer System** or **Shared Computer System** that might cause or contribute to a **Claim**;

b. costs or expenses incurred to update, restore, replace, upgrade, maintain, or improve any **Computer System**; or

c. penalties of any nature, however denominated, arising by contract.

Incident means **Cyber Incident** or **Media Incident**.

Insured means:

1. the **Named Insured**;
2. any **Subsidiary** of the **Named Insured**, but only with respect to **Incidents** which occur while it is a **Subsidiary**;
3. any past, present, or future natural person principal, partner, officer, director, trustee, employee, leased employee or temporary employee of an **Organization**, but only with respect to an **Incident** committed within the scope of such natural person's duties performed on behalf of such **Organization**;
4. any past, present or future independent contractor of an **Organization** who is a natural person, agent, or single person entity, but only with respect to the commission of an **Incident** within the scope of such natural person's, agent's, or single person entity's duties, performed on behalf of such **Organization**; or
5. any past, present or future natural person intern or volunteer worker of an **Organization** and who is registered or recorded as an intern or volunteer worker with such **Organization**, but only with respect to an **Incident** within the scope of such natural person's duties performed on behalf of such **Organization**.

Insured's Computer System means a **Computer System** leased, owned or operated by an **Insured** or operated solely for the benefit of an **Insured** by a third party under written contract with an **Insured**.

Insurer means the insurance company providing this insurance.

Interrelated Incidents means all **Incidents** that have as a common nexus any act, fact, circumstance, situation, event, transaction, cause or series of related acts, facts, circumstances, situations, events, transactions or causes.

Interruption in Service means a detectable interruption or degradation in service of:

1. with respect to Insuring Agreement B1, an **Insured's Computer System**; or
2. with respect to Insuring Agreement B2, a **Shared Computer System**;

caused by a **Malicious Computer Act**.

Malicious Computer Act means malicious or fraudulent:

1. unauthorized access to or use of a **Computer System**;
2. alteration, corruption, damage, manipulation, misappropriation, theft, deletion, or destruction of **Digital Data**;
3. creation, transmission, or introduction of a computer virus or harmful code into a **Computer System**; or
4. restriction or inhibition of access, including denial of service attacks, upon or directed against a **Computer System**.

Media Content means any data, text, sounds, images, graphics, music, photographs, or advertisements, and shall include video, streaming content, webcasts, podcasts, blogs, online forums, and chat rooms. **Media Content** shall not include computer software, software technology, or the actual goods, products or services described, illustrated or displayed in such **Media Content**.

Media Incident means any error, misstatement, misleading statement, act, omission, neglect or breach of duty actually or allegedly committed or attempted by any **Insured**, or by any person or entity for whom an **Insured** is legally responsible, in the public display of:

1. **Media Content** on an **Insured's** website or printed material; or
2. **Media Content** posted by or on behalf of an **Insured** on any social media site or anywhere on the Internet,

which results in the following:

a. copyright infringement, passing-off, plagiarism, piracy, or misappropriation of property rights;

b. infringement or dilution of title, logo, slogan, domain name, metatag, trademark, trade name, service mark, or service name;

c. defamation, libel, slander, or any other form of defamation or harm to the character, reputation or feelings of any person or entity, including product disparagement, trade libel, outrage, infliction of emotional distress, or *prima facie* tort;

d. invasion or infringement of the right of privacy or publicity, including the torts of intrusion upon seclusion, publication of private facts, false light, or misappropriation of name or likeness;

e. false arrest, detention or imprisonment, harassment, trespass, wrongful entry or eviction, eavesdropping, or other invasion of the right of private occupancy;

f. improper deep linking or framing; or

g. unfair competition or unfair trade practices, including misrepresentations in advertising, solely when alleged in conjunction with the alleged conduct referenced in items a–f immediately above.

Named Insured means the entity shown in Item 1 of the Declarations.

Network Extortion Threat means any credible threat or series of related threats directed at an **Insured** to:

1. release, divulge, disseminate, destroy or use **Protected Information** or confidential corporate information of an **Insured** taken from an **Insured** as a result of the unauthorized access to or unauthorized use of an **Insured's Computer System** or **Shared Computer System**;

2. cause a **Network Security Failure**;

3. alter, corrupt, damage, manipulate, misappropriate, delete or destroy **Digital Data**; or

4. restrict or inhibit access to an **Insured's Computer System** or **Shared Computer System**;

where the **Insured** makes a payment or a series of payments, or otherwise meets a demand, in exchange for the mitigation or removal of such threat or series of related threats.

Network Security means those activities performed by an **Insured**, or by others on behalf of an **Insured**, to protect an **Insured's Computer System** or **Shared Computer System**.

Network Security Failure means a failure in **Network Security**, including the failure to prevent a **Malicious Computer Act**.

Non-Panel Response Provider means any firm providing the services shown in the definition of **Cyber Incident Response Expenses** to an **Insured** that is not a **Pre-Approved Response Provider**.

Organization means the **Named Insured** and any **Subsidiary**.

Payment Card means an authorized account, or evidence of an account, for a credit card, debit card, charge card, fleet card or stored value card between the **Payment Card Brand** and its customer.

Payment Card Brand means any payment provider whose payment method is accepted for processing, including Visa Inc. International, MasterCard Worldwide, Discover Financial Services, American Express Company, and JCB International.

Payment Card Industry Data Security Standards means the rules, regulations, standards or guidelines adopted or required by the **Payment Card Brand** or the Payment Card Industry Data Security Standards Council relating to data security and the safeguarding, disclosure and handling of **Protected Information**.

Payment Card Loss means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries which an **Insured** becomes legally obligated to pay as a result of an **Insured's** actual or alleged failure:

1. of **Network Security**; or

2. to properly protect, handle, manage, store, destroy, or otherwise control **Payment Card** data, including **Protected Information**,

where such amount is determined pursuant to a payment card processing agreement between an **Organization** and a **Payment Card Brand**, or a merchant agreement between an **Organization** and a payment services provider, including for mobile payment services, or demanded in writing from an issuing or acquiring bank that processes **Payment Card** transactions, due to an **Insured's** actual or alleged non-compliance with applicable **Payment Card Industry Data Security Standards**, EMV specifications, or mobile payment security requirements. **Payment Card Loss** shall not include:

1. subsequent fines or assessments for continued non-compliance with the **Payment Card Industry Data Security Standards,** EMV Specifications, or a mobile payment services merchant agreement; or
2. costs or expenses incurred to update or improve privacy or network security controls, policies or procedures to a level beyond that which existed prior to the applicable **Cyber Incident** or to be compliant with applicable **Payment Card Industry Data Security Standards,** EMV Specifications, or a mobile payment services merchant agreement.

Period of Restoration means the continuous period of time that:

1. begins with the earliest date of an **Interruption in Service**; and
2. ends on the date when an **Insured's Computer System** or **Shared Computer System** is or could have been repaired or restored with reasonable speed to the same functionality and level of service that existed prior to the **Interruption in Service**. In no event shall the **Period of Restoration** exceed sixty (60) days.

Policy means, collectively, the Declarations, **Application,** this policy form and any endorsements attached hereto.

Policy Period means the period of time shown in Item 2 of the Declarations, unless changed pursuant to Section XV, Termination of this Policy.

Pollutants means any solid, liquid, gaseous or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals, asbestos, asbestos products or waste. Waste includes materials to be recycled, reconditioned or reclaimed.

Pre-Approved Response Provider means any firm listed on the **Insurer's** pre-approved service provider list available on request from the **Insurer** or on the pre-approved service provider list specified on the website shown in Item 9A of the Declarations.

Privacy or Cyber Laws means any local, state, federal, and foreign identity theft and privacy protection laws, legislation, statutes, or regulations that require commercial entities that collect **Protected Information** to post privacy policies, adopt specific privacy or security controls, or notify individuals in the event that **Protected Information** has potentially been compromised.

Property Damage means physical injury to, or loss or destruction of, tangible property, including the loss of use thereof whether or not it is damaged or destroyed.

Protected Information means the following, in any format:

1. a natural person's name, e-mail address, social security number, medical or healthcare data, other protected health information, driver's license number, state identification number, credit card number, debit card number, address, unpublished telephone number, account number, account histories, personally identifiable photos, personally identifiable videos, Internet browsing history, biometric records, passwords or other non-public personal information as defined in any **Privacy or Cyber Laws**; or
2. any other third party confidential or proprietary information:
   a. provided to an **Insured** and protected under a nondisclosure agreement or similar contract; or
   b. which an **Organization** is legally responsible to maintain in confidence.

Regulatory Fines means any civil monetary fine or penalty imposed by a federal, state, local or foreign governmental entity in such entity's regulatory or official capacity as a result of a **Regulatory Proceeding**. **Regulatory Fines** shall not include any civil monetary fines or penalties that are not insurable by law, criminal fines, disgorgement, or the multiple portion of any multiplied damage award.

Regulatory Proceeding means a suit, civil investigation or civil proceeding by or on behalf of a government agency, government licensing entity, or regulatory authority, commenced by the service of a complaint or similar pleading based on an alleged or potential violation of **Privacy or Cyber Laws** as a result of a **Cyber Incident**, and which may reasonably be expected to give rise to a **Claim** under Insuring Agreement E.

Retroactive Date means the date shown in Item 5 of the Declarations.

Shared Computer System means a **Computer System**, other than an **Insured's Computer System**, operated for the benefit of an **Insured** by a third party under written contract with an **Insured**, including data hosting, cloud services or computing, co-location, data back-up, data storage, data processing, platforms, software, and infrastructure-as-a-service.

Subsidiary means:

1. any entity while more than fifty percent (50%) of the outstanding securities representing the present right to vote for election of or to appoint directors, trustees, managers, members of the Board of Managers or equivalent positions of such entity are owned, or controlled, by the **Named Insured,** directly or through one or more **Subsidiaries**;
2. any entity formed as a partnership while more than fifty percent (50%) of the ownership interests representing the present right to vote for election of or to appoint the management or executive committee members or equivalent positions of such entity are owned, or controlled, by the **Named Insured,** directly or through one or more **Subsidiaries**; or
3. any entity while:
   a. exactly fifty percent (50%) of the voting rights representing the present right to vote for election of or to appoint directors, trustees, managers, members of the Board of Managers or equivalent positions of such entity are owned, or controlled, by the **Named Insured,** directly or through one of more **Subsidiaries**; and
   b. the **Named Insured,** pursuant to a written contract with the owners of the remaining and outstanding voting stock of such entity, solely controls the management and operation of such entity.

Telephone Fraud Financial Loss means toll and line charges which an **Insured** incurs, solely as a result of the fraudulent infiltration and manipulation of the **Insured's Telephone System** from a remote location to gain access to outbound long distance telephone service.

Telephone System means PBX, CBX, Merlin, VoIP, remote access (including DISA), and all related peripheral equipment or similar systems owned or leased by an **Insured** for purposes of voice-based telecommunications.

Trade Secret means information, including a formula, pattern, compilation, program, device, method, technique or process, that derives actual or potential economic value from not being generally known to or readily ascertainable by other persons who can obtain value from its disclosure or use, so long as reasonable efforts have been made to maintain its secrecy.

Waiting Period means the number of hours shown in Item 4 of the Declarations.

III. EXCLUSIONS

A. EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS

The **Insurer** shall not be liable for **Costs**, **Damages**, or **Claims Expenses** on account of any **Incident** or any **Claim**:

1. Conduct

   alleging, based upon, arising out of or attributable to:

   a. any dishonest, fraudulent, criminal, malicious or intentional act, error or omission, or any intentional or knowing violation of the law by an **Insured**; or
   b. the gaining in fact of any profit, remuneration or financial advantage to which any **Insured** was not legally entitled.

However, this exclusion shall not apply to **Claims Expenses** or the **Insurer's** duty to defend any such **Claim**, until there is a final, non-appealable adjudication against, binding arbitration against, adverse admission by, finding of fact against, or plea of *nolo contendere* or no contest by, the **Insured** as to such conduct or violation, at which time the **Insured** shall reimburse the **Insurer** for any **Claims Expenses** paid by the **Insurer**. Provided that:

i. no conduct pertaining to any natural person **Insured** shall be imputed to any other natural person **Insured**; and

ii. any conduct pertaining to any past, present, or future **Control Group Member**, other than a Rogue Actor, shall be imputed to an **Organization**. For purposes of this exclusion, "Rogue Actor" means a **Control Group Member** acting outside his or her capacity as such.

2. Prior Knowledge

alleging, based upon, arising out of or attributable to any **Incident** that first occurred, arose or took place prior to the earlier of the effective date of this **Policy**, or the effective date of any **Policy** issued by the **Insurer** of which this **Policy** is a continuous renewal or a replacement, and any **Control Group Member** knew of such **Incident**; and, with respect to Insuring Agreements E and F, any **Control Group Member** reasonably could have foreseen that such **Incident** did or could lead to a **Claim**.

3. Pending or Prior Proceedings

alleging, based upon, arising out of, or attributable to:

a. any pending or prior litigation, **Claim**, demand, arbitration, administrative or regulatory proceeding or administrative or regulatory investigation filed or commenced on or before the Pending or Prior Proceedings Date shown in Item 6 of the Declarations, or alleging or derived from the same or substantially the same fact, circumstance or situation underlying or alleged therein; or

b. any other **Incident** whenever occurring which, together with an **Incident** underlying or alleged in any pending or prior litigation, **Claim**, demand, arbitration, administrative or regulatory proceeding or administrative or regulatory investigation as set forth pursuant to paragraph a. immediately above, would constitute **Interrelated Incidents**.

4. Prior Notice

alleging, based upon, arising out of, or attributable to:

a. any **Incident**, fact, circumstance or situation which has been the subject of any written notice given and accepted under any other policy before the effective date of this **Policy**; or

b. any other **Incident** whenever occurring which, together with an **Incident** which has been the subject of such notice, would constitute **Interrelated Incidents**.

5. Bodily Injury

for any **Bodily Injury**. However, solely with respect to Insuring Agreement E and Insuring Agreement F, this exclusion shall not apply to mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock resulting from an **Incident**.

6. Property Damage

alleging, based upon, arising out of, or attributable to **Property Damage**.

7. Pollution

alleging, based upon, arising out of or attributable to the actual, alleged or threatened discharge, release, escape, seepage, migration, or disposal of **Pollutants**, or any direction or request that any **Insured** test for, monitor, clean up, remove, contain, treat, detoxify or neutralize **Pollutants**, or any voluntary decision to do so.

8. Infrastructure Outage

alleging, based upon, arising out of or attributable to any electrical or mechanical failure or interruption, electrical disturbance, surge, spike, brownout, blackout, or outages to electricity, gas, water, Internet access service provided by the Internet service provider that hosts an **Insured's** website, telecommunications or other infrastructure. However, this exclusion shall not apply to failures, interruptions, disturbances or outages of telephone, cable or telecommunications systems, networks or infrastructure:

a. under an **Insured's** operational control which are a result of a **Network Security Failure**;

b. solely with respect to Insuring Agreement B, which are the result of a **Cyber Incident** impacting a **Shared Computer System**; or

c. solely with respect to Insuring Agreement E, which are the result of a **Cyber Incident**.

9. War

alleging, based upon, arising out of or attributable to war, invasion, acts of foreign enemies, terrorism, hijacking, hostilities or warlike operations (whether war is declared or not), military or usurped power, civil commotion assuming the proportions of or amounting to an uprising, strike, lock-out, riot, civil war, rebellion, revolution, or insurrection. However, this exclusion shall not apply to an **Act of Cyber-Terrorism** that results in a **Cyber Incident**.

10. Nuclear

alleging, based upon, arising out of or attributable to the planning, construction, maintenance, operation or use of any nuclear reactor, nuclear waste, storage or disposal site, or any other nuclear facility, the transportation of nuclear material, or any nuclear reaction or radiation, or radioactive contamination, regardless of its cause.

11. Contract

for breach of any express, implied, actual or constructive contract, warranty, guarantee, or promise, including any actual or alleged liability assumed by an **Insured**, unless such liability would have attached to the **Insured** even in the absence of such contract, warranty, guarantee, or promise. However, this exclusion shall not apply to:

a. solely with respect to Insuring Agreement E, **Payment Card Loss**;

b. solely with respect to Insuring Agreements A or E, an **Insured's** contractual obligation to maintain the confidentiality or security of third party personal or corporate information; or

c. solely with respect to Insuring Agreement F, misappropriation of idea under implied contract.

12. Fees or Chargebacks

alleging, based upon, arising out of or attributable to:

a. any fees, expenses, or costs paid to or charged by an **Insured**; or

b. chargebacks, chargeback fees, interchange fees or rates, transfer fees, transaction fees, discount fees, merchant service fees, or prospective service fees.

However, solely with respect to Insuring Agreement E, this exclusion shall not apply to **Payment Card Loss**.

13. Intellectual Property

alleging, based upon, arising out of or attributable to any infringement of, violation of, misappropriation of, or assertion of any right to or interest in a patent or **Trade Secret** by any **Insured**. However, solely with respect to Insuring Agreement E, this exclusion shall not apply to a **Claim** arising out of the actual or alleged disclosure or theft of **Protected Information** resulting from a **Network Security Failure**.

14. Antitrust or Unfair Trade Practices

alleging, based upon, arising out of or attributable to any price fixing, restraint of trade, monopolization, interference with economic relations (including interference with contractual relations or with prospective advantage), unfair competition, unfair business or unfair trade practices, or any violation of the Federal Trade Commission Act, the Sherman Anti-Trust Act, the Clayton Act, or any other federal statutory provision involving anti-trust, monopoly, price fixing, price discrimination, predatory pricing, restraint of trade, unfair competition, unfair business or unfair trade practices, and any amendments thereto or any rules or regulations promulgated thereunder, amendments thereof, or any similar federal, state, or common law. However, this exclusion shall not apply to:

a. solely with respect to Insuring Agreement E, a **Claim** resulting directly from a violation of **Privacy or Cyber Laws**; or

b. solely with respect to Insuring Agreement F, a **Claim** for a **Media Incident** as defined in paragraph g of such definition.

15. Consumer Protection Laws

alleging, based upon, arising out of or attributable to any violation by an **Insured** of the Truth in Lending Act, Fair Debt Collection Practices Act, or the Fair Credit Reporting Act or any amendments thereto or any rules or regulations promulgated thereunder, including the Fair and Accurate Credit Transactions Act, and any amendments thereto or any rules or regulations promulgated thereunder, amendments thereof, or any similar federal, state or common law. However, solely with respect to Insuring Agreement E, this exclusion shall not apply to a **Claim** arising out of the actual or alleged disclosure or theft of **Protected Information** resulting from a **Cyber Incident**.

16. ERISA or Securities Law Violation

alleging, based upon, arising out of or attributable to an **Insured's** violation of:

a. the Employee Retirement Income Security Act of 1974, as amended;

b. the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisors Act, or any other federal, state or local securities law,

and any amendments thereto or any rules or regulations promulgated thereunder, amendments thereof, or any similar federal, state or common law. However, solely with respect to Insuring Agreements A or E, paragraph a, immediately above, shall not apply.

17. Discrimination or Employment Practices

alleging, based upon, arising out of or attributable to any illegal discrimination of any kind, or any employment relationship, or the nature, terms or conditions of employment, including claims for workplace torts, wrongful termination, dismissal or discharge, or any discrimination, harassment, breach of employment contract or defamation. However, solely with respect to Insuring Agreement E, this exclusion shall not apply to that part of any **Claim** alleging employee-related invasion of privacy or employee–related wrongful infliction of emotional distress in the event such **Claim** arises out of the actual or alleged disclosure or theft of **Protected Information** resulting from a **Cyber Incident**.

18. Unsolicited Communications

alleging, based upon, arising out of or attributable to any unsolicited electronic dissemination of faxes, e-mails or other communications by or on behalf of an **Insured**, including actions brought under the Telephone Consumer Protection Act, any federal or state anti-spam statutes, or any other federal or state statute, law, rule, regulation or common law relating to a person's or entity's right of seclusion. However, solely with respect to Insuring Agreement E, this exclusion shall not apply to a **Claim** resulting from a **Cyber Incident** as defined under subparagraph 1(c) of such definition.

19. Unlawful Use or Collection of Protected Information

alleging, based upon, arising out of or attributable to the unlawful use or collection of **Protected Information**, or the failure to provide adequate notice that such information is being collected or used, by an **Insured**, with knowledge of any **Control Group Member**.

20. Intentional Failure to Disclose

alleging, based upon, arising out of or attributable to an **Insured's** intentional failure to disclose the loss of **Protected Information** in violation of any law or regulation. However, this exclusion will not apply when an **Insured's** failure to disclose occurs pursuant to an order from a law enforcement or government authority in the course of a criminal investigation. Solely with respect to Insuring Agreement E, only facts pertaining to and knowledge possessed by any **Control Group Member** shall be imputed to other **Insureds**.

B. EXCLUSIONS APPLICABLE TO SPECIFIC INSURING AGREEMENTS

In addition to the Exclusions in Section IIIA above, the **Insurer** shall not be liable for **Costs**, **Damages**, or **Claims Expenses** on account of any **Incident** or any **Claim**:

1. Force Majeure

solely with respect to Insuring Agreements B and C, alleging, based upon, arising out of or attributable to fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God (which does not include acts by actors purporting to be God), nature or any other physical event, however caused and whether contributed to, made worse by, or in any way results from any such events. This exclusion applies regardless of any other contributing or aggravating cause or event that contributes concurrently with or in any sequence to the **Costs**, **Damages**, or **Claims Expenses** on account of any **Incident** or any **Claim**.

2. Governmental Authority

solely with respect to Insuring Agreements C and D, alleging, based upon, arising out of, or attributable to any action of a public or governmental authority, including the seizure, confiscation or destruction of an **Insured's Computer System**, a **Shared Computer System** or an **Insured's Digital Data**.

3. Insured v. Insured

solely with respect to Insuring Agreements E and F, brought or maintained by, on behalf of, or in the right of any **Insured**. Provided, however, solely with respect to Insuring Agreement E, this exclusion shall not apply to that part of any **Claim** alleging employee-related invasion of privacy or employee–related wrongful infliction of emotional distress in the event such **Claim** arises out of the loss of **Protected Information** resulting from a **Cyber Incident**.

4. Licensing Entities

solely with respect to Insuring Agreement F, alleging, based upon, arising out of or attributable to any action brought by or on behalf of the Federal Trade Commission, the Federal Communications Commission, or any other federal, state, or local government agency or ASCAP, SESAC, BMI or other licensing or rights entities in such entity's regulatory, quasi-regulatory, or official capacity, function or duty.

5. False Advertising or Misrepresentation

solely with respect to Insuring Agreement F, alleging, based upon, arising out of or attributable to any inaccurate, inadequate, or incomplete description of the price of goods, products or services, disclosure of fees, representations with respect to authenticity of any product, or the failure of any goods, product or services to conform with advertised quality or performance.

6. Contest or Game of Chance

solely with respect to Insuring Agreement F, alleging, based upon, arising out of or attributable to any gambling, contest, game of chance or skill, lottery, or promotional game, including tickets or coupons or over-redemption related thereto.

IV. SPOUSES, COMMON LAW PARTNERS, ESTATES AND LEGAL REPRESENTATIVES

Coverage under this **Policy** shall extend to any **Claim** for any **Incident** made against:

A. the lawful spouse or domestic partner of a natural person **Insured** solely by reason of such spouse's or domestic partner's status as a spouse or domestic partner, or such spouse's or domestic partner's ownership interest in property which the claimant seeks as recovery in such **Claim**; or

B. the estate, heirs, legal representatives or assigns of a natural person **Insured** if such natural person **Insured** is deceased, or the legal representatives or assigns of a natural person **Insured** if such natural person **Insured** is legally incompetent, insolvent or bankrupt,

provided that:

1. no coverage is provided for any act, error, or omission of an estate, heir, legal representative, assign, spouse or domestic partner; and
2. all of the terms and conditions of this **Policy** including, without limitation, all applicable Retentions shown in Item 4 of the Declarations apply to such **Claim**.

V. EXTENDED REPORTING PERIOD

A. Solely with respect to Insuring Agreements A, E, and F, if the **Insurer** terminates or does not renew this **Policy** (other than for failure to pay a premium when due), or if the **Named Insured** terminates or does not renew this **Policy** and does not obtain replacement coverage as of the effective date of such termination or nonrenewal, the **Named Insured** shall have the right, upon payment of the additional premium shown in Item 7A of the Declarations and subject to the terms specified in Subsections B-E directly below, to a continuation of the coverage granted by this **Policy** for an **Extended Reporting Period** shown in Item 7B of the Declarations following the effective date of such termination or non-renewal.

B. Coverage for the **Extended Reporting Period** shall be only for **Claims** first made or **Incidents** first discovered during such **Extended Reporting Period** and arising from **Incidents** taking place prior to the effective date of such termination or non-renewal. This right to continue coverage shall lapse unless written notice of such election is given by the **Named Insured** to the **Insurer**, and the **Insurer** receives payment of the additional premium shown in Item 7A of the Declarations, within thirty (30) days following the effective date of termination or non-renewal.

C. The **Extended Reporting Period** is non-cancelable and the entire premium for the **Extended Reporting Period** shall be deemed fully earned and non-refundable upon payment.

D. The **Extended Reporting Period** shall not increase or reinstate any Limits of Insurance. The Limits of Insurance as shown in Item 3 and Item 4 of the Declarations shall apply to both the **Policy Period** and the **Extended Reporting Period**, combined.

E. A change in **Policy** terms, conditions, exclusions or premiums shall not be considered a non-renewal for purposes of triggering the rights to the **Extended Reporting Period**.

VI. LIMITS OF INSURANCE

Regardless of the number of Insuring Agreements purchased under this **Policy**, or the number of **Incidents**, **Insureds** against whom **Claims** are brought, **Claims** made or persons or entities making **Claims**:

A. MAXIMUM POLICY AGGREGATE LIMIT OF INSURANCE

The **Insurer's** maximum limit of insurance under all Insuring Agreements resulting from all **Claims** first made and **Incidents** first discovered during the **Policy Period** is shown in Item 3B of the Declarations, Maximum Policy Aggregate Limit of Insurance.

B. AGGREGATE LIMIT FOR ALL INCIDENTS OR CLAIMS UNDER ANY ONE INSURING AGREEMENT

The **Insurer's** maximum limit of insurance for all **Incidents** or **Claims** under any one Insuring Agreement shall be the applicable Aggregate Limit for all **Incidents** or **Claims** shown in Item 4 of the Declarations,

which shall be part of, and not in addition to, the Maximum Policy Aggregate Limit of Insurance shown in Item 3B of the Declarations.

C. MAXIMUM LIMIT OF INSURANCE FOR EACH INCIDENT OR CLAIM UNDER ANY ONE INSURING AGREEMENT

The **Insurer's** maximum limit of insurance for each **Incident** or **Claim** under any one Insuring Agreement shall be the applicable Each **Incident** or **Claim** Limit shown in Item 4 of the Declarations, which shall be part of, and not in addition to, the applicable Aggregate Limit for all **Incidents** or **Claims** shown in Item 4 of the Declarations, and the Maximum Policy Aggregate Limit of Insurance shown in Item 3B of the Declarations.

D. MAXIMUM LIMIT OF INSURANCE FOR ALL INTERRELATED INCIDENTS AND CLAIMS

All **Claims** arising out of the same **Incident** and all **Interrelated Incidents** shall be deemed to be one **Claim**, and such **Claim** shall be deemed to be first made on the date the earliest of such **Claims** is first made, regardless of whether such date is before or during the **Policy Period**.

All **Interrelated Incidents** shall be deemed to be one **Incident**, and such **Incident** shall be deemed to be first discovered, on the date the earliest of such **Incidents** is first discovered, regardless of whether such date is before or during the **Policy Period**.

The maximum limit of insurance for all **Interrelated Incidents** and **Claims** arising out of such **Interrelated Incidents** shall be the Maximum Single **Incident** or **Claim** Limit of Insurance shown in Item 3A of the Declarations, regardless of whether **Costs**, **Damages** or **Claims Expenses** from a single **Incident** or **Claim** are covered under more than one Insuring Agreement. Notwithstanding anything in this paragraph to the contrary, in no event shall the **Insurer** pay more than the applicable:

1. Maximum Policy Aggregate Limit of Insurance shown in Item 3B of the Declarations,
2. Aggregate Limit for all **Incidents** or **Claims** under any one Insuring Agreement shown in Item 4 of the Declarations, and
3. Each **Incident** or **Claim** Limit under any one Insuring Agreement shown in Item 4 of the Declarations.

E. **Costs**, **Damages** and **Claims Expenses** shall be part of and not in addition to the applicable Limit of Insurance shown in the Declarations, and shall reduce such applicable Limit of Insurance. If the applicable Limit of Insurance is exhausted by payment of **Costs**, **Damages** and **Claims Expenses**, the obligations of the **Insurer** under this **Policy** shall be completely fulfilled and extinguished.

F. Any sub-limits shown in the Declarations or added by endorsement to this **Policy** shall be part of and not in addition to the applicable Limit of Insurance shown in the Declarations, and shall reduce such applicable Limit of Insurance.

VII. RETENTION

A. The liability of the **Insurer** shall apply only to that part of **Costs**, **Damages**, and **Claims Expenses** which is in excess of the applicable Retention amount shown in Item 4 of the Declarations. Such Retention shall be borne uninsured by the **Named Insured** and at the risk of all **Insureds**.

B. With respect to Insuring Agreement B, the **Insurer** will pay the actual **Business Interruption Loss**, **Contingent Business Interruption Loss** and **Extra Expenses** incurred by an **Insured**:

1. once the applicable **Waiting Period** shown in Item 4B of the Declarations has expired; and
2. which is in excess of the applicable Retention amount shown in Item 4B of the Declarations.

The **Waiting Period** and Retention amounts shall be computed as of the start of the **Interruption in Service**.

Any **Business Interruption Loss** or **Contingent Business Interruption Loss** incurred by an **Insured** during the **Waiting Period**, and resulting from an **Interrelated Incident** with **Extra Expenses**, shall reduce and may exhaust any applicable Retention.

C. A single Retention amount shall apply to **Costs**, **Damages**, and **Claims Expenses**, arising from all **Incidents** or **Claims** alleging an **Interrelated Incident**.

D. If a single **Incident** or **Claim**, or **Interrelated Incidents** are subject to different Retentions, the applicable Retention shall be applied separately to each part of the **Costs, Damages,** and **Claim Expenses**, but the sum of such Retentions shall not exceed the largest applicable Retention.

VIII. NOTICE

A. Urgent crisis management assistance by the **Cyber Incident Response Coach** is available at the hotline number shown in the Declarations. Use of the services of the **Cyber Incident Response Coach** for a consultation DOES NOT constitute notice under this **Policy** of a **Cyber Incident** or **Claim**. In order to provide notice under this **Policy**, such notice must be given in accordance with and is subject to Subsections B-D of this Section VIII.

B. An **Insured** shall, as a condition precedent to such **Insured's** rights under this **Policy**, give to the **Insurer** written notice of any **Incident** or **Claim** as soon as practicable after any **Control Group Member** discovers such **Incident** or becomes aware of such **Claim**, but in no event later than:

1. if this **Policy** expires (or is otherwise terminated) without being renewed with the **Insurer**, ninety (90) days after the effective date of such expiration or termination; or
2. the expiration of the **Extended Reporting Period**, if applicable,

provided that if the **Insurer** sends written notice to the **Named Insured**, stating that this **Policy** is being terminated for nonpayment of premium, an **Insured** shall give to the **Insurer** written notice of such **Claim** prior to the effective date of such termination.

C. If, during the **Policy Period**, any **Control Group Member** first becomes aware of any specific **Incident** which may reasonably give rise to a future **Claim** under this **Policy**, and written notice is given to the **Insurer** during the **Policy Period**, of the:

1. nature of the **Incident**;
2. identity of the **Insureds** allegedly involved;
3. circumstances by which the **Insureds** first became aware of the **Incident**;
4. identity of the actual or potential claimants;
5. foreseeable consequences of the **Incident**; and
6. nature of the potential **Damages**;

then any **Claim** which arises out of such **Incident** shall be deemed to have been first made at the time such written notice was received by the **Insurer**. The **Insurer** will not pay for **Damages** or **Claims Expenses** incurred prior to the time such **Incident** results in a **Claim**.

D. All notices under any provision of this **Policy** shall be given as follows:

1. Notice to the **Insureds** may be given to the **Named Insured** at the address shown in Item 1 of the Declarations.
2. Notice to the **Insurer** of any **Incident** or **Claim** shall be given to the **Insurer** at the physical address or email address shown in Item 9A of the Declarations.
3. All other notices to the **Insurer** under this **Policy** shall be given to the **Insurer** at the physical address shown in Item 9B of the Declarations.

Notice given as set out above shall be deemed to be received and effective upon actual receipt thereof by the addressee, or one day following the date such notice is sent, whichever is earlier. When any such notices are sent to a physical address, such notices shall be sent by prepaid express courier or certified mail properly addressed to the appropriate party.

IX. DEFENSE AND SETTLEMENT

A. Except as provided in Subsection B of this Section IX, the **Insurer** shall have the right and duty to defend any **Claim** brought against an **Insured** even if such **Claim** is groundless, false or fraudulent.

The **Insurer** shall consult and endeavor to reach an agreement with the **Insured** regarding the appointment of counsel, but shall retain the right to appoint counsel and to make such investigation and defense of a **Claim** as it deems necessary.

B. The **Insurer** shall have the right, but not the duty, to defend any **Regulatory Proceeding**. For such **Claims**, the **Insured** shall select defense counsel from the **Insurer's** list of approved law firms, and the **Insurer** reserves the right to associate in the defense of such **Claims**.

C. No **Insured** shall settle any **Claim**, incur any **Claims Expenses**, or otherwise assume any contractual obligation or admit any liability with respect to any **Claim** without the **Insurer's** written consent, which shall not be unreasonably withheld.

D. The **Insurer** shall not settle any **Claim** without the written consent of the **Named Insured**. If the **Named Insured** refuses to consent to a settlement recommended by the **Insurer** and acceptable to the claimant, then the **Insurer's** applicable Limit of Insurance under this **Policy** with respect to such **Claim** shall be reduced to:

1. the amount of **Damages** for which the **Claim** could have been settled plus all **Claims Expenses** incurred up to the time the **Insurer** made its recommendation to the **Named Insured**; plus

2. eighty percent (80%) of all subsequent covered **Damages** and **Claims Expenses** in excess of such amount referenced in paragraph (1) immediately above, which amount shall not exceed that portion of any applicable Limit of Insurance that remains unexhausted by payment of **Costs**, **Damages**, and **Claims Expenses**. The remaining twenty percent (20%) of all subsequent covered **Damages** and **Claims Expenses** shall be borne by the **Insureds** uninsured and at their own risk. However, this provision does not apply to any potential settlement that is within the Retention.

E. The **Insurer** shall not be obligated to investigate, defend, pay or settle, or continue to investigate, defend, pay or settle any **Claim** after any applicable Limit of Insurance has been exhausted by payment of **Costs**, **Damages**, or **Claims Expenses**, or by any combination thereof, or after the **Insurer** has deposited the remainder of any unexhausted applicable Limit of Insurance into a court of competent jurisdiction. In either such case, the **Insurer** shall have the right to withdraw from the further investigation, defense, payment or settlement of such **Claim** by tendering control of such **Claim** to the **Insured**.

F. The **Insureds** shall cooperate with the **Insurer** and provide to the **Insurer** all information and assistance which the **Insurer** reasonably requests including attending hearings, depositions and trials and assistance in effecting settlements, securing and giving evidence, obtaining the attendance of witnesses and conducting the defense of any **Claim** covered by this **Policy**. The **Insured** shall do nothing that may prejudice the **Insurer's** position. The **Insureds** shall immediately forward to the **Insurer**, at the address shown in Item 9A of the Declarations, every demand, notice, summons, or other process or pleading received by an **Insured** or its representatives.

G. With the exception of paragraph 6 of the **Cyber Incident Response Expenses** definition, an **Insured** has the right to incur **Cyber Incident Response Expenses** without the **Insurer's** prior consent. However, the **Insurer** shall, at its sole discretion and in good faith, pay only for such expenses that the **Insurer** deems to be reasonable and necessary.

X. PROOF OF LOSS FOR FIRST PARTY INSURING AGREEMENTS

A. Requests for payment or reimbursement of **Costs** incurred by an **Insured** shall be accompanied by a proof of loss with full particulars as to the computation of such **Costs**. Such proof of loss will include in detail how the **Costs** were calculated, and what assumptions have been made, and shall include documentary evidence, including any applicable reports, books of accounts, bills, invoices and other vouchers or proofs of payment made by an **Insured** in relation to such **Costs**. Furthermore, the **Insureds** shall cooperate with, and provide any additional information reasonably requested by, the **Insurer** in its review of **Costs**, including the right to investigate and audit the proof of loss and inspect the records of an **Insured**.

B. With respect to Insuring Agreement B, the **Business Interruption Loss** or **Contingent Business Interruption Loss** will be determined taking full account and due consideration of an **Insured's** proof of loss and in addition, the trends or circumstances which affect the profitability of the business and would have affected the profitability of the business had the **Business Interruption Loss** or **Contingent Business Interruption Loss** not occurred, including all material changes in market conditions or adjustment expenses which would affect the net profit generated. However, the **Insurer's** adjustment will not include the **Insured's** increase in income that would likely have been earned as a result of an increase in the volume of business due to favorable business conditions caused by the impact of a **Malicious Computer Act** on others.

XI. ALLOCATION

If a **Claim** includes both covered and uncovered matters, then coverage shall apply as follows:

A. **Claims Expenses**: One hundred percent (100%) of **Claims Expenses** incurred by any **Insured** on account of such **Claim** shall be considered covered provided that the foregoing shall not apply with respect to: (i) a **Regulatory Proceeding**; or, (ii) any **Insured** for whom coverage is excluded pursuant to Exclusion III.A.1 or Section XIV, Subsection C. With respect to a **Regulatory Proceeding**, amounts for covered **Claims Expenses** and for uncovered fees, costs and expenses shall be allocated based upon the relative legal and financial exposures of, and the relative benefits obtained by, the parties to such matters.

B. Loss other than **Claims Expenses**: all remaining loss incurred by such **Insured** from such **Claim** shall be allocated between covered **Damages** and uncovered damages based upon the relative legal and financial exposures of, and the relative benefits obtained by, the parties to such matters.

XII. OTHER INSURANCE

If any **Costs, Damages** or **Claims Expenses** covered under this **Policy** are covered under any other valid and collectible insurance, then this **Policy** shall cover such **Costs, Damages** or **Claims Expenses,** subject to the **Policy** terms and conditions, only to the extent that the amount of such **Costs, Damages** or **Claims Expenses** are in excess of the amount of such other insurance whether such other insurance is stated to be primary, contributory, excess, contingent or otherwise, unless such other insurance is written only as specific excess insurance over the Limits of Insurance provided by this **Policy**.

XIII. MATERIAL CHANGES IN EXPOSURE

A. ACQUISITION OR CREATION OF ANOTHER ENTITY

If, during the **Policy Period**, the **Named Insured**:

1. acquires voting securities in another entity or creates another entity, which as a result of such acquisition or creation becomes a **Subsidiary**; or
2. acquires any entity by merger into or consolidation with the **Named Insured**;

then, subject to the terms and conditions of this **Policy**, such entity and its natural person **Insureds** shall be covered under this **Policy** but only with respect to **Claims** for **Incidents,** or **Incidents**, as applicable, taking place after such acquisition or creation, unless the **Insurer** agrees to provide coverage by endorsement for **Claims** for **Incidents,** or **Incidents**, as applicable, taking place prior to such acquisition or creation.

B. ACQUISITION OF THE NAMED INSURED

If, during the **Policy Period**, any of the following events occurs:

1. the acquisition of the **Named Insured**, or of all or substantially all of its assets, by another entity, or the merger or consolidation of the **Named Insured** into or with another entity such that the **Named Insured** is not the surviving entity; or
2. the obtaining by any person, entity or affiliated group of persons or entities of the right to elect, appoint or designate at least fifty percent (50%) of the directors, trustees, managers, members of the Board of Managers, management or executive committee members or equivalent positions of the **Named Insured**;

then coverage under this **Policy** will continue in full force and effect until termination of this **Policy**, but only with respect to **Claims** for **Incidents,** or **Incidents**, as applicable, taking place before such event. Coverage under this **Policy** will cease as of the effective date of such event with respect to **Claims** for **Incidents,** or **Incidents**, as applicable, taking place after such event. This **Policy** may not be cancelled after the effective time of the event, and the entire premium for this **Policy** shall be deemed earned as of such time.

C. TERMINATION OF A SUBSIDIARY

If, before or during the **Policy Period,** an entity ceases to be a **Subsidiary**, coverage with respect to such **Subsidiary** and any **Insured** (as defined in paragraphs 3, 4 and 5 of such definition) of the **Subsidiary** shall continue until termination of this **Policy**. Such coverage continuation shall apply only with respect to **Claims** for **Incidents,** or **Incidents**, as applicable, taking place prior to the date such entity ceased to be a **Subsidiary**.

XIV. REPRESENTATIONS

A. In granting coverage to any **Insured**, the **Insurer** has relied upon the declarations and statements in the **Application** for this **Policy**. Such declarations and statements are the basis of the coverage under this **Policy** and shall be considered as incorporated in and constituting part of this **Policy**.

B. The **Application** for coverage shall be construed as a separate **Application** for coverage by each **Insured**. With respect to the declarations and statements in such **Application**, no knowledge possessed by a natural person **Insured** shall be imputed to any other natural person **Insured**.

C. However, in the event that such **Application** contains any misrepresentations made with the actual intent to deceive or contains misrepresentations which materially affect either the acceptance of the risk or the hazard assumed by the **Insurer** under this **Policy**, then no coverage shall be afforded for any **Incident** or **Claim** based upon, arising from or in consequence of any such misrepresentations with respect to:

   1. any natural person **Insured** who knew of such misrepresentations (whether or not such natural person knew such **Application** contained such misrepresentations); or

   2. an **Organization**, if any past or present **Control Group Member** knew of such misrepresentations (whether or not such **Control Group Member** knew such **Application** contained such misrepresentations).

D. The **Insurer** shall not be entitled under any circumstances to void or rescind this **Policy** with respect to any **Insured**.

XV. TERMINATION OF THIS POLICY

A. This **Policy** shall terminate at the earliest of the following times:

   1. the effective date of termination specified in a prior written notice by the **Named Insured** to the **Insurer**;

   2. sixty (60) days after receipt by the **Named Insured** of a written notice of termination from the **Insurer** for any reason allowed by applicable insurance laws or regulations, other than failure to pay premium when due;

   3. twenty (20) days after receipt by the **Named Insured** of a written notice of termination from the **Insurer** for failure to pay a premium when due, unless the premium is paid within such twenty (20) day period;

   4. upon expiration of the **Policy Period** as shown in Item 2 of the Declarations; or

   5. at such other time as may be agreed upon by the **Insurer** and the **Named Insured**.

B. If the **Policy** is terminated by the **Named Insured** or the **Insurer**, the **Insurer** shall refund the unearned premium computed *pro rata*. Payment or tender of any unearned premium by the **Insurer** shall not be a condition precedent to the effectiveness of such termination, but such payment shall be made as soon as practicable.

XVI. TERRITORY AND VALUATION

A. Coverage provided under this **Policy** shall extend to **Incidents** and **Claims** taking place, brought or maintained anywhere in the universe. Any provision in this **Policy** pertaining to coverage for **Incidents** or **Claims** made or **Damages** or **Claims Expenses** sustained anywhere outside the United States of America shall only apply where legally permissible.

B. All premiums, limits, retentions, **Costs, Damages, Claims Expenses** and other amounts under this **Policy** are expressed and payable in the currency of the United States of America. If judgment is rendered, settlement is denominated or another element of loss under this **Policy** is stated in a currency other than United States of America dollars, or if **Extortion Expenses** are stated in a currency, including Bitcoin or other crypto-currency(ies), other than United States of America dollars, payment under this **Policy** shall be made in United States dollars at the applicable rate of exchange as published in *The Wall Street Journal* as of the date the final judgment is reached, the amount of the settlement is agreed upon or the other element of loss is due, respectively, or, if not published on such date, the next date of publication of *The Wall Street Journal*. If there is no applicable rate of exchange published in the Wall Street Journal, then payment under this **Policy** shall be made in the equivalent of United States of America dollars at the actual rate of exchange for such currency.

XVII. CYBER INCIDENT RESPONSE FUND PROVISIONS

A. With respect to the **Cyber Incident Response Team** or a **Non-Panel Response Provider**:

1. The **Insureds** are under no obligation to contract for services with the **Cyber Incident Response Team**. However, if an **Insured** elects to use any **Non-Panel Response Providers** for any **Cyber Incident Response Expenses**, the applicable Limits of Insurance shown in Item 4A2 of the Declarations will apply.

2. The **Insurer** shall not be a party to any agreement entered into between any **Cyber Incident Response Team** service provider and an **Insured**.

3. **Cyber Incident Response Team** service providers are independent contractors, and are not agents of the **Insurer**. The **Insureds** agree that the **Insurer** assumes no liability arising out of any services rendered by a **Cyber Incident Response Team** service provider. The **Insurer** shall not be entitled to any rights or subject to any obligations or liabilities set forth in any agreement entered into between any **Cyber Incident Response Team** service provider and an **Insured**. Any rights and obligations with respect to such agreement, including billings, fees and services rendered, are solely for the benefit of, and borne solely by such **Cyber Incident Response Team** service provider and such **Insured**, and not the **Insurer**.

4. The **Insurer** has no obligation to provide any of the services provided by the **Cyber Incident Response Team**.

B. With respect to any other third party vendor, the **Insurer** may provide the **Named Insured** with a list of third-party privacy and network security loss mitigation vendors whom the **Named Insured**, at its own election and at the **Named Insured's** own expense, may retain for cyber risk management to inspect, assess, and audit the **Named Insured's** property, operations, systems, books, and records, including the **Named Insured's** network security, employee cyber security awareness, incident response plans, services provider contracts, and regulatory compliance. Any loss mitigation inspection, assessment, or audit purchased by the **Named Insured**, and any report or recommendation resulting therefrom, shall not constitute an undertaking at the request of or for the benefit of the **Insurer**.

XVIII. SUBROGATION

A. The **Insurer** shall have no rights of subrogation against any **Insured** under this **Policy** unless Exclusion III.A.1 or Section XIV, Subsection C, applies.

B. In the event of payment under this **Policy**, the **Insureds** must transfer to the **Insurer** any applicable rights to recover from another person or entity all or part of any such payment. The **Insureds** shall execute all papers required and shall do everything necessary to secure and preserve such rights, including the execution of such documents necessary to enable the **Insurer** to effectively bring suit or otherwise pursue subrogation rights in the name of the **Insureds**.

C. If prior to the **Incident** or **Claim** connected with such payment an **Insured** has agreed in writing to waive such **Insured's** right of recovery or subrogation against any person or entity, such agreement shall not be considered a violation of such **Insured's** duties under this **Policy**.

XIX. ACTION AGAINST THE INSURER AND BANKRUPTCY

Except as provided in Section XXII, Alternative Dispute Resolution, no action shall lie against the **Insurer**. No person or entity shall have any right under this **Policy** to join the **Insurer** as a party to any action against any **Insured** to determine the liability of such **Insured** nor shall the **Insurer** be impleaded by any **Insured** or its legal representatives. Bankruptcy or insolvency of any **Insured** or of the estate of any **Insured** shall not relieve the **Insurer** of its obligations nor deprive the **Insurer** of its rights or defenses under this **Policy**.

XX. AUTHORIZATION CLAUSE

By acceptance of this **Policy**, the **Named Insured** agrees to act on behalf of all **Insureds** with respect to the giving of notice of **Incident** or **Claim**, the giving or receiving of notice of termination or non-renewal, the payment of premiums, the receiving of any premiums that may become due under this **Policy**, the agreement to and acceptance of endorsements, consenting to any settlement, exercising the right to the **Extended Reporting Period**, and the giving or receiving of any other notice provided for in this **Policy**, and all **Insureds** agree that the **Named Insured** shall so act on their behalf.

XXI. ALTERATION, ASSIGNMENT, AND HEADINGS

A. Notice to any agent or knowledge possessed by any agent or by any other person shall not affect a waiver or a change in any part of this **Policy** nor prevent the **Insurer** from asserting any right under the terms of this **Policy**.

B. No change in, modification of, or assignment of interest under this **Policy** shall be effective except when made by a written endorsement to this **Policy** which is signed by an authorized representative of the **Insurer**.

C. The titles and headings to the various parts, sections, subsections and endorsements of the **Policy** are included solely for ease of reference and do not in any way limit, expand, serve to interpret or otherwise affect the provisions of such parts, sections, subsections or endorsements.

D. Any reference to the singular shall include the plural and vice versa.

XXII. ALTERNATIVE DISPUTE RESOLUTION

A. The **Insureds** and the **Insurer** shall submit any dispute or controversy arising out of or relating to this **Policy** or the breach, termination or invalidity thereof to the alternative dispute resolution ("ADR") process set forth in this Section.

B. Either an **Insured** or the **Insurer** may elect the type of ADR process discussed below. However, such **Insured** shall have the right to reject the choice by the **Insurer** of the type of ADR process at any time prior to its commencement, in which case the choice by such **Insured** of ADR process shall control.

C. There shall be two choices of ADR process:

   1. non-binding mediation administered by any mediation facility to which the **Insurer** and an **Insured** mutually agree, in which such **Insured** and the **Insurer** shall try in good faith to settle the dispute by mediation in accordance with the then-prevailing commercial mediation rules of the mediation facility; or

   2. arbitration submitted to any arbitration facility to which an **Insured** and the **Insurer** mutually agree, in which the arbitration panel shall consist of three disinterested individuals.

   In either mediation or arbitration, the mediator or arbitrators shall have knowledge of the legal, corporate management, or insurance issues relevant to the matters in dispute. In the event of arbitration, the decision of the arbitrators shall be final and binding and provided to both parties, and the award of the arbitrators shall not include attorneys' fees or other costs. In the event of mediation, either party shall have the right to commence a judicial proceeding. However, no such judicial proceeding shall be commenced until at least sixty (60) days after the date the mediation shall be deemed concluded or terminated. In all events, each party shall share equally the expenses of the ADR process.

D. Either ADR process may be commenced in New York or in the state shown in Item 1 of the Declarations as the principal address of the **Named Insured**. The **Named Insured** shall act on behalf of each and every **Insured** in connection with any ADR process under this Section.

XXIII. INTERPRETATION

The terms and conditions of this **Policy** shall be interpreted and construed in an even-handed fashion as between the parties. If the language of this **Policy** is deemed to be ambiguous or otherwise unclear, the issue shall be resolved in the manner most consistent with the relevant terms and conditions, without regard to authorship of the language, without any presumption or arbitrary interpretation or construction in favor of either the **Insureds** or the **Insurer**, and without reference to the reasonable expectations of either the **Insureds** or the **Insurer**.

XXIV. COMPLIANCE WITH TRADE SANCTIONS

This insurance does not apply to the extent that trade or economic sanctions or other similar laws or regulations prohibit the providing of such insurance.

General Enhancement Endorsement – Cyber

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy

It is agreed that the **Policy** is amended as follows:

1. Section II, DEFINITIONS, is amended as follows:

   A. Paragraph 3 of the definition of **Claim** is deleted and replaced with the following;

      3. arbitration, mediation, or other alternative dispute resolution proceeding against any **Insured** seeking monetary damages or non-monetary or injunctive relief, commenced by the receipt of a written demand, or service of a complaint or similar pleading;

   B. The definition of **Computer System** is deleted and replaced with the following:

      Computer System means computer hardware, software, **Telephone System**, firmware, and the data stored thereon, as well as associated input and output devices, data storage devices, mobile devices, networking equipment and storage area network or other electronic data backup facilities. The terms referenced herein include Industrial Control Systems.

   C. Paragraph 2 of the definition of **Cyber Incident Response Expenses** is deleted and replaced with the following:

      2. retaining the services of third party forensic firms, including a Payment Card Industry (PCI) Forensic Investigator, to determine the cause and scope of a **Cyber Incident**;

   D. Paragraph 5.c. of the definition of **Cyber Incident Response Expenses** is deleted and replaced with the following:

      c. call center services, mailing services or costs, and other related services for notification as required by law; or

   E. The definition of **Cyber Incident Response Team** is amended by replacing the term "**Pre-Approved Service Providers**" with "**Pre-Approved Response Providers**".

   F. The definition of **Damages** is amended by inserting the phrase "**Regulatory Fines,**" after "**Payment Card Loss,**".

   G. Paragraph 2 of the definition of **Damages** is amended by inserting the word "directly" before "imposed".

   H. The definition of **Network Extortion Threat** is deleted and replaced with the following:

      Network Extortion Threat means any credible threat or series of related threats directed at an **Insured** to:

      1. release, divulge, disseminate, destroy or use **Protected Information**, or confidential corporate information of an **Insured**, as a result of the unauthorized access to or unauthorized use of an **Insured's Computer System** or **Shared Computer System**;
      2. cause a **Network Security Failure**;
      3. alter, corrupt, damage, manipulate, misappropriate, encrypt, delete or destroy **Digital Data**; or
      4. restrict or inhibit access to an **Insured's Computer System** or **Shared Computer System**;

      where a demand is made for the **Insured** to make a payment or a series of payments, or otherwise meet a demand, in exchange for the mitigation or removal of such threat of series of related threats.

      Furthermore, **Network Extortion Threat** includes a threat or series of related threats connected to any of the acts above that have already commenced.

I. The definition of **Payment Card Loss** is deleted and replaced with the following:

Payment Card Loss means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries, including card reissuance costs, which an **Insured** becomes legally obligated to pay as a result of an **Insured's** actual or alleged failure:

1. of **Network Security**; or
2. to properly protect, handle, manage, store, destroy, or otherwise control **Payment Card** data, including **Protected Information**;

where such amount is determined pursuant to a payment card processing agreement between an **Organization** and a **Payment Card Brand**, or a merchant agreement between an **Organization** and a payment services provider, including for mobile payment services, or demanded in writing from an issuing or acquiring bank that processes **Payment Card** transactions, due to an **Insured's** actual or alleged non-compliance with applicable **Payment Card Industry Data Security Standards**, EMV specifications, or mobile payment security requirements. **Payment Card Loss** shall not include:

1. subsequent fines or assessments for non-compliance with the **Payment Card Industry Data Security Standards**, EMV Specifications, or a mobile payment services merchant agreement unrelated to a specific **Claim**; or
2. costs or expenses incurred to update or improve privacy or network security controls, policies or procedures to a level beyond that which existed prior to the applicable **Cyber Incident** or to be compliant with applicable **Payment Card Industry Data Security Standards**, EMV Specifications, or a mobile payment services merchant agreement.

J. The definition of **Pre-Approved Response Provider** is amended by replacing both instances of the word "service" with "response".

K. The definition of **Property Damage** is deleted and replaced with the following:

Property Damage means physical injury to, or destruction of, tangible property, including the resulting loss of use thereof.

L. The definition of **Protected Information** is amended by deleting the word "unpublished".

M. The definition of **Protected Information** is further amended by deleting Paragraph 2.a. and replacing it with the following:

a. that is not available to or known by the general public; or

N. The definition of **Regulatory Proceeding** is amended by inserting ", notice," after "complaint".

O. The definition of **Retroactive Date** is amended by adding the following:

If Item 5 of the Declarations is left blank or contains the phrases "Full Prior Acts", "N/A", "Not Applicable", or "None", then **Retroactive Date** means the beginning of time.

2. Section III, EXCLUSIONS, subsection A, EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS, is amended as follows:

A. Exclusion 1. Conduct is amended by deleting the word "dishonest".

B. Exclusion 3. Pending or Prior Proceedings, paragraph a., is amended by inserting the word "written" before "demand".

C. Exclusion 4. Prior Notice is deleted and replaced with the following:

4. Prior Notice

alleging, based upon, arising out of, or attributable to:

a. any **Incident**, fact, circumstance or situation which has been the subject of any written notice given and accepted under any other policy of which this **Policy** is a direct or indirect renewal or replacement; or

b. any other **Incident**, whenever occurring, which, together with an **Incident** which has been the subject of such notice pursuant to paragraph a. immediately above, would constitute **Interrelated Incidents**.

D. Exclusion 11. Contract is deleted and replaced with the following:

11. Contract

for breach of any express, implied, actual or constructive contract, warranty, guarantee, or promise, including any actual or alleged liability assumed by an **Insured**, unless such liability would have attached to the **Insured** even in the absence of such contract, warranty, guarantee, or promise. However, this exclusion shall not apply to:

a. an **Insured's** contractual obligation to maintain the confidentiality or security of **Protected Information**;

b. an unintentional violation by an **Insured** to comply with an **Organization's** Privacy Policy;

c. solely with respect to Insuring Agreement E, **Payment Card Loss**; or

d. solely with respect to Insuring Agreement F, misappropriation of idea under implied contract.

E. Exclusion 13. Intellectual Property is deleted and replaced with the following:

13. Intellectual Property

alleging, based upon, arising out of or attributable to any infringement of, violation of, misappropriation of, or assertion of any right to or interest in a patent or **Trade Secret** by any **Insured**. However, this exclusion shall not apply to:

a. solely with respect to Insuring Agreements A-D, the actual or alleged theft of a third party's **Trade Secret** resulting from a **Cyber Incident**; provided, however, this exclusion shall still nevertheless apply to any **Costs**, **Damages** or **Claims Expenses** on account of any **Cyber Incident** or **Claim** for the economic or market value of **Trade Secrets**; or

b. solely with respect to Insuring Agreement E, any **Claim** arising out of the actual or alleged disclosure or theft of **Protected Information** resulting from a **Network Security Failure**.

F. Exclusion 16. ERISA or Securities Law Violation is deleted and replaced with the following:

16. Securities Law Violation

alleging, based upon, arising out of or attributable to an **Insured's** violation of the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisors Act, or any other federal, state or local securities law, and any amendments thereto or any rules or regulations promulgated thereunder, amendments thereof, or any similar federal, state or common law.

G. The last sentence of Exclusion 18. Unsolicited Communications is deleted and replaced with the following:

However, solely with respect to Insuring Agreement E, this exclusion shall not apply to a **Claim** resulting from a **Cyber Incident** as defined under subparagraphs 1(a) or 1(c) of such definition.

H. Exclusion 19. Unlawful Use or Collection of Protected Information is deleted and replaced with the following:

19. Unlawful Use or Collection of Protected Information

alleging, based upon, arising out of or attributable to:

a. the unlawful collection or unlawful intentional use of **Protected Information**; or

b. the failure to provide adequate notice that **Protected Information** is being collected or used,

by an **Insured**, with knowledge of any **Control Group Member** at the time of the **Incident**.

I. Exclusion 20. Intentional Failure to Disclose is deleted.

3. Section VII, RETENTION, is amended by deleting subsection B and replacing it with the following:

   B. With respect to Insuring Agreement B, the **Insurer** will pay:

      1. the actual **Business Interruption Loss** and **Contingent Business Interruption Loss** incurred by an **Insured**:

         a. once the applicable **Waiting Period** shown in Item 4B of the Declarations has expired; and

         b. which is in excess of the applicable Retention amount shown in Item 4B of the Declarations;

         and

      2. **Extra Expenses** incurred by an **Insured**:

         a. as of the start of the **Interruption In Service**; and

         b. which are in excess of the applicable Retention amount showed in Item 4B of the Declarations.

   The **Waiting Period** and Retention amounts shall be computed as of the start of the **Interruption in Service**.

   Any **Business Interruption Loss, Contingent Business Interruption Loss**, or **Extra Expenses** incurred by an **Insured** during the **Waiting Period** shall reduce and may exhaust any applicable Retention.

4. Section VIII, NOTICE, is amended at subsection B by adding the following at the end thereof:

   If the **Insured** is unable to provide notification required under this **Policy** due a prohibition by any law enforcement or governmental authority, the **Insured** will use its best efforts to provide the **Insurer** with information to make the **Insurer** aware of a potential or actual **Incident** or **Claim** until written notice can actually be provided. Notwithstanding the foregoing, there shall be no coverage for any such **Incident** or **Claim** if the information withheld relating to such **Incident** or **Claim** was:

   a. both (i) known to the **Insured** prior to the **Policy** Inception Date set forth in Item 2 of the Declarations, and (ii) not disclosed in the **Application**; or

   b. not disclosed in writing to the **Insurer** within a reasonable time period after the prohibition on disclosing the information was revoked or no longer necessary.

5. Section XV, TERMINATION OF THIS POLICY, is amended by deleting Paragraph A.2.

6. Section XXIII, INTERPRETATION, is deleted.

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

Cyber Incident Response Fund Side-Car

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that solely with respect to Insuring Agreement A, **Cyber Incident Response Fund**, Section VI, Limits of Insurance, subsections B and C, are deleted in their entirety and replaced with the following:

B. AGGREGATE LIMIT FOR ALL INCIDENTS UNDER ANY ONE INSURING AGREEMENT

The **Insurer's** maximum limit of insurance for all **Cyber Incidents** under Insuring Agreement A shall be the applicable Aggregate Limit for all **Cyber Incidents** shown in Item 4A of the Declarations, which shall be in addition to, and not part of, the Maximum Policy Aggregate Limit of Insurance shown in Item 3B of the Declarations.

C. MAXIMUM LIMIT OF INSURANCE FOR EACH INCIDENT UNDER ANY ONE INSURING AGREEMENT

The **Insurer's** maximum limit of insurance for each **Cyber Incident** under Insuring Agreement A shall be the applicable Each **Cyber Incident** Limit shown in Item 4A of the Declarations, which shall be in addition to, and not part of, the Maximum Policy Aggregate Limit of Insurance shown in Item 3B of the Declarations, but nevertheless part of, and not in addition to, the applicable Aggregate Limit for all **Cyber Incidents** shown in Item 4A of the Declarations.

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

© 2016

Extended Period of Attrition Endorsement

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that the **Policy** is amended as follows:

1. Section I, INSURING AGREEMENTS, First Party Insuring Agreements, subsection B, Business Interruption and Extra Expenses, is deleted and replaced with the following:

   B. *BUSINESS INTERRUPTION AND EXTRA EXPENSES*

   The **Insurer** will pay:

   1. the **Business Interruption Loss** and **Extra Expenses** incurred by an **Insured** during the **Period of Restoration** resulting directly from a **Cyber Incident** which first occurs during the **Policy Period**, plus any resulting **Customer Attrition Loss** incurred by the **Insured** during the **Period of Attrition**; and

   2. the **Contingent Business Interruption Loss** and **Extra Expenses** incurred by an **Insured** during the **Period of Restoration** resulting directly from a **Cyber Incident** which first occurs during the **Policy Period.**

2. Section II, DEFINITIONS, is amended as follows:

   A. The definition of **Costs** is amended by adding the following:

   - **Customer Attrition Loss.**

   B. The following definitions are added:

   - **Customer Attrition Loss** means:

     1. the **Insured's** net profit before income taxes that would have been earned had no **Interruption in Service** occurred, only if such difference can be proven by a quantifiable reduction in customers and seasonally-adjusted daily revenue amounts caused by damage to the **Insured's** reputation as a direct result of the **Interruption in Service**;

     2. with the **Insurer's** prior consent, costs incurred by an **Insured** to retain the services of a third party forensic accounting firm to determine the amount of **Customer Attrition Loss**;

     provided that the **Insured** provides written evidence that the **Customer Attrition Loss** is a direct result of an **Interruption in Service** under Insuring Agreement B.1.

     Customer Attrition Loss shall not include:

     1. loss arising out of the diminution in value of money, securities, property or any other item of value;

     2. loss arising out of any liability to any third party as a result of a **Cyber Incident**, including **Damages**;

     3. loss arising out of unfavorable business conditions, loss of market value or any other consequential loss;

     4. **Claims Expenses**;

     5. **Cyber Incident Response Expenses**;

     6. **Extra Expenses**; or

     7. wages, salaries or other compensation of directors, officers, similar executives, or employees of any **Insured**.

- **Period of Attrition** means the continuous period of time that:
  1. begins with the date which immediately follows the last date of the **Period of Restoration**; and
  2. ends on the earliest date that the **Insured's** customer counts and seasonally-adjusted daily revenue amounts recover to the same level that would have existed had there been no **Interruption in Service**, so long as such recovery is subsequently sustained on an average daily basis over the course of at least ten business days. In no event shall the **Period of Attrition** exceed days(60) days.

3. Section VI, LIMITS OF INSURANCE, is amended by adding the following:

- MAXIMUM LIMIT OF INSURANCE FOR CUSTOMER ATTRITION LOSS RESULTING FROM AN INTERRUPTION IN SERVICE

  A. Subject to Section VI, LIMITS OF INSURANCE, the **Insurer's** maximum limit of insurance for all **Customer Attrition Loss** resulting directly from an **Interruption in Service** under Insuring Agreement B.1. shall be:

[$1000000] (the "Interruption in Service Customer Attrition Sublimit").

  This Interruption in Service Customer Attrition Sublimit shall be part of and not in addition to:

  a. the Each **Cyber Incident** Limit; and

  b. the Aggregate Limit for all **Cyber Incidents**,

  set forth in Item 4.B.1. of the Declarations for this **Policy**.

  The Interruption in Service Customer Attrition Sublimit shall also be part of and not in addition to the Maximum Policy Aggregate Limit of Insurance set forth in Item 3B of the Declarations and will in no way serve to increase the **Insurer's** maximum liability under the **Policy**. The **Insurer's** obligation to reimburse **Customer Attrition Loss** because of an **Interruption in Service** under Insuring Agreement B.1. is in excess of the **Insured's** applicable Retention amount as set forth in Item 4.B.1., and once the applicable **Waiting Period** shown in Item 4.B.1. of the Declarations, has expired.

  B. Notwithstanding the foregoing, if the field above in paragraph A of this subsection is left blank or N/A is shown, then the Limits of Insurance shown in Item 4.B.1. of the Declarations shall apply to the sum of all **Customer Attrition Loss** resulting directly from an **Interruption in Service**.

  C. There shall be no coverage for **Customer Attrition Loss** as a direct result of an **Interruption in Service** other than with respect to Insuring Agreement B.1.

4. Section X, PROOF OF LOSS FOR FIRST PARTY INSURING AGREEMENTS, subsection B, is deleted and replaced with the following:

  B. With respect to Insuring Agreement B, the **Business Interruption Loss**, **Contingent Business Interruption Loss**, and **Customer Attrition Loss** will be determined taking full account and due consideration of an **Insured's** proof of loss and in addition, the trends or circumstances which affect the profitability of the business and would have affected the profitability of the business had the **Business Interruption Loss**, **Contingent Business Interruption Loss**, or **Customer Attrition Loss** not occurred, including all material changes in market conditions or adjustment expenses which would affect the net profit generated, as well as income derived from substitute methods, facilities, or personnel used by the **Insured** to maintain its revenue stream. However, the **Insurer's** adjustment will not include the **Insured's** increase in income that would likely have been earned as a result of an increase in the volume of business due to favorable business conditions caused by the impact of a **Malicious Computer Act** on others.

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

Cyber Crime Endorsement

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that solely with respect to the coverage provided by this endorsement, the **Policy** is amended as follows:

1. Item 4. of the Declarations is amended to include the following:

Cyber Crime Insuring Agreements	Each Loss Limit of Insurance	Aggregate Limit of Insurance	Each Loss Retention
☐ Funds Transfer Fraud Limit of Insurance	$ <SLL_FTF>	$ <AGG_FTF>	$ <RET_FTF>
☐ Computer Fraud Limit of Insurance	$ <SLL_CF>	$ <AGG_CF>	$ <RET_CF>
☐ Social Engineering Fraud Limit of Insurance	$ <SLL_SEF>	$ <AGG_SEF>	$ <RET_SEF>

2. Section I, INSURING AGREEMENTS, is amended by adding the following:

CYBER CRIME INSURING AGREEMENTS

Funds Transfer Fraud

The **Insurer** will pay for loss of **Money** or **Securities** sustained by an **Insured** resulting directly from **Funds Transfer Fraud** committed by a third party which is **Discovered** during the **Policy Period.**

Computer Fraud

The **Insurer** will pay the **Insured** for loss of **Money, Securities** or **Property** sustained by an **Insured** resulting directly from **Computer Fraud** committed by a third party which is **Discovered** during the **Policy Period.**

Social Engineering Fraud

The **Insurer** shall pay the **Insured** for loss of **Money** or **Securities** sustained by an **Insured** resulting directly from **Social Engineering Fraud** committed by a person purporting to be a **Vendor, Client** or an **Employee** who was authorized by the **Insured** to instruct other **Employees** to transfer **Money** or **Securities** which is **Discovered** during the **Policy Period.**

Hereinafter, the above Insuring Agreements shall be collectively referred to as the "Cyber Crime Insuring Agreements".

3. Section II, DEFINITIONS, is amended to include the following:

Client means a customer of an **Organization** to whom such **Organization** provides goods or services under written contract or for a fee.

Computer Fraud means the unlawful taking of **Money, Securities** or **Property** resulting from a **Computer Violation.**

Computer Violation means the unauthorized entry into, or transmission of corrupting or harmful software code into the **Insured's Computer System** which is directed against an **Insured**.

Cryptocurrency means a digital or electronic medium of exchange, operating independently of a central bank, in which encryption techniques are used to regulate the generation of units and to verify the transfer of such units.

Discovery or Discovered means knowledge acquired by a **Control Group Member** of an **Insured** which would cause a reasonable person to believe a covered loss has occurred or an occurrence has arisen that may subsequently result in a covered loss. This includes loss:

1. sustained prior to the inception date of any coverage under this endorsement;
2. which does not exceed the Retention set forth in in Item 4. of the Declarations; or
3. the exact amount or details of which are unknown.

Employee means any natural person in the regular service of an **Insured** in the ordinary course of such **Insured's** business, whom such **Insured** governs and directs in the performance of such service, including a part-time, seasonal, leased and temporary employee, intern or volunteer. Any natural person that otherwise meets the foregoing definition shall be considered an **Employee** even if such person's title is that of partner, principal, director, officer, or if such person is a **Control Group Member**.

Funds Transfer Fraud means fraudulent electronic, telegraphic, cable, teletype, facsimile, telephone or written instructions (other than forgery), purportedly issued by an **Insured**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Insured** at such institution, without such **Insured's** knowledge or consent.

Money means currency, coin, bank notes and bullion. However, **Money** does not mean **Securities** or any **Cryptocurrency**.

Official Authorization means a valid signature of an actual **Employee** or an electronic record of entry and approval into a wire transfer system, accounting system, or similar system which is capable of maintaining and reproducing an audit trail which demonstrates that an actual **Employee** approved a transaction within their authority. A forgery is not an **Official Authorization**. **Official Authorization** shall not include a typed name in any form (including but not limited to email, letterhead or pre-printed material), but shall include electronic reproductions of hand-written signatures in any form.

Property means any tangible property other than **Money** and **Securities**. **Property** does not include **Digital Data**.

Securities means negotiable and nonnegotiable instruments or contracts representing either **Money** or property including revenue and other stamps (whether represented by actual stamps or unused value in a meter) in current use, casino chips, tokens and tickets, provided that **Securities** does not include **Money** or any **Cryptocurrency**.

Social Engineering Fraud means the intentional misleading of an **Employee**, through misrepresentation of a material fact which is relied upon by an **Employee**, believing it be genuine which results in the transferring, payment or delivery of **Money** or **Securities**.

Vendor means any entity or natural person that has provided goods or services to an **Insured** under a legitimate pre-existing arrangement or written agreement. However, **Vendor** does not include any financial institution, asset manager, broker-dealer, armored motor vehicle **Insurer**, or any similar entity.

4. The definition of **Insured** set forth in Section II, DEFINITIONS, is deleted and replaced with the following:

Insured means the **Named Insured** and its **Subsidiaries**.

5. Section III, EXCLUSIONS, is deleted and replaced with the following:

A. No coverage will be available for:

1. loss due to kidnap, ransom or any other extortion payment surrendered to any person as a result of a threat to do bodily harm to any person or a threat to do damage to any property;

2. loss involving:

a. the disclosure of an **Insured's** or another entity or person's confidential or personal information while in the care, custody or control of an **Insured**, including but not limited to patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any similar type of non-public information;

b. loss involving the use of another entity or person's confidential or personal information while in the care, custody or control of an **Insured**, including but not limited to patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any similar type of non-public information; or

c. fees, costs, fines, penalties or any other expenses incurred by an **Insured** which result, directly or indirectly, from the access to or disclosure of another entity or person's confidential or personal information, including but not limited to patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any similar type of nonpublic information,

provided that this Exclusion 2. a. and b. shall not apply to loss that is otherwise covered under any Cyber Crime Insuring Agreement;

3. loss or damage due to declared or undeclared war, civil war, insurrection, rebellion, revolution, military, naval or usurped power, governmental intervention, expropriation or nationalization, or any act or condition incident to any of the foregoing;

4. loss or damage due to nuclear reaction, nuclear radiation or radioactive contamination, or any act or condition incident to any of the foregoing;

5. loss of income not realized as the result of a covered loss;

6. indirect or consequential loss of any kind;

7. fees, costs or expenses incurred or paid in defending or prosecuting any legal proceeding or claim;

8. loss sustained by one **Insured** to the advantage of any other **Insured**;

9. loss or damage due to **Computer Fraud** or **Funds Transfer Fraud** or other fraudulent, dishonest or criminal act committed by any authorized representative of an **Insured**, whether acting alone or in collusion with others.

B. With respect to the Funds Transfer Fraud and Computer Fraud Insuring Agreements, no coverage will be available for loss resulting from any transfer, payment or delivery of **Money**, **Securities** or **Property** approved by an **Employee**, or arising out of any misrepresentation received by any **Employee**, agent, independent contractor or other representative of the **Insured**, whether such transfer, payment or delivery was made in good faith or as a result of trick, artifice, fraud or false pretenses.

C. With respect to the Social Engineering Fraud Insuring Agreement, the **Insurer** shall not be liable for:

1. loss or damage to **Money** or **Securities** as a result of **Computer Fraud** or **Funds Transfer Fraud**;

2. loss due to any investment in **Securities**, or ownership in any corporation, partnership, real property, or similar instrument, whether or not such investment is genuine;

3. loss due to the failure of any party to perform, in whole or in part, under any contract;

4. loss due to the extension of any loan, credit or similar promise to pay;

5. loss due to any party's use of or acceptance of any credit card, debit card or similar instrument, whether or not genuine;

6. loss due to any person purporting to be a representative of any financial institution, asset manager, broker-dealer, armored motor vehicle company, or any similar entity;

7. loss of **Money** or **Securities** while in the mail or in the custody of any carrier for hire, including but not limited to any armored motor vehicle company;

8. loss due to the failure, malfunction, inadequacy or illegitimacy of any product or service;

9. loss of or damage to any **Property**;

10. loss due to any gambling, game of chance, lottery or similar game;

11. loss in excess of $50,000, unless the transferring, payment or delivery of **Money** or **Securities** is made:
    a. by a **Control Group Member**, or
    b. by any **Employee** (other than a **Control Group Member**), agent, independent contractor or other representative of the **Insured**, after receiving **Official Authorization** from:
        i. a **Control Group Member**, or
        ii. an **Employee** acting in a supervisory capacity.

D. In addition to the amended Section III, no coverage will be available for:

1. loss unless sustained by any **Insured** at any time, and **Discovered** during the **Policy Period** and prior to the termination of the coverage provided by this endorsement as to such **Insured**;
2. loss unless sustained by any **Insured** at any time, and **Discovered** during the **Policy Period** and prior to the termination of any Cyber Crime Insuring Agreement or any particular coverage offered under any Cyber Crime Insuring Agreement;
3. loss unless sustained by any **Insured** at any time, and **Discovered** during the **Policy Period** and prior to the termination of the coverage provided by this endorsement in its entirety,

provided that in no event will coverage be available under this coverage for such loss if such loss is covered under any renewal or replacement of this coverage or any Cyber Crime Insuring Agreement or any particular coverage offered under any Cyber Crime Insuring Agreement.

6. Section V, EXTENDED REPORTING PERIOD, is deleted.

7. Section VI, LIMITS OF INSURANCE, is deleted and replaced with the following:

The **Insurer** will pay for loss sustained by an **Insured** at any time and **Discovered** during the **Policy Period**.

The **Insurer's** maximum liability for each loss shall not exceed the limit of insurance applicable to such loss, as set forth in Item 4 of the Declarations for this **Policy**, as amended by this endorsement, regardless of the number of **Insureds** sustaining such loss.

The **Insurer's** maximum liability shall not exceed the limit of insurance:

1. Applicable to the Funds Transfer Fraud Insuring Agreement: for all loss or losses resulting from any act, casualty or event, any series of related acts, casualties or events, or any act or series of acts committed by one natural person or entity, or in which the same group of natural persons or entities acting together are implicated, regardless of whether such act, casualty or event or series of acts, casualties or events was committed or occurred before or during the **Policy Period**.
2. Applicable to the Computer Fraud Insuring Agreement: for all loss or losses resulting from any act, casualty or event, any series of related acts, casualties or events, or any act or series of acts committed

by one natural person or entity, or in which the same group of natural persons or entities acting together are implicated, regardless of whether such act, casualty or event or series of acts, casualties or events was committed or occurred before or during the **Policy Period**.

3. Applicable to the Social Engineering Fraud Insuring Agreement: for all loss or losses resulting from any act, casualty or event, any series of related acts, casualties or events, or any act or series of acts committed by one natural person or entity, or in which the same group of natural persons or entities acting together are implicated, regardless of whether such act, casualty or event or series of acts, casualties or events was committed or occurred before or during the **Policy Period**.

If a loss is covered under more than one Cyber Crime Insuring Agreement, the maximum amount payable under this **Policy** shall not exceed the largest applicable limit of insurance of any such Cyber Crime Insuring Agreement.

The **Insurer's** total cumulative liability for all loss **Discovered** during the **Policy Period** shall not exceed the applicable Cyber Crime Aggregate Limit of Insurance as set forth in Item 4. of the Declarations. Such amount shall be part of and not in addition to the Maximum Policy Aggregate Limit of Insurance as stated in Item 3. of the Declarations. Each payment made under the terms of this endorsement shall reduce the unpaid portion of the applicable Cyber Crime Aggregate Limit of Insurance and the Maximum Policy Aggregate Limit of Insurance until they are exhausted.

On exhausting the applicable Cyber Crime Aggregate Limit of Insurance by such payments the **Insurer** shall have no further liability for loss or losses regardless of when **Discovered** and whether or not previously reported to the **Insurer**; and the unpaid portion of the applicable Cyber Crime Aggregate Limit of Insurance and Maximum Policy Aggregate Limit of Insurance shall not be increased or reinstated by any recovery made and applied in accordance with Section XVIII. Recoveries (as amended in paragraph 17 of this endorsement). In the event that a loss of **Securities** is settled by indemnity in lieu of payment, then such loss shall not reduce the unpaid portion of the applicable Cyber Crime Aggregate Limit of Insurance or Maximum Policy Aggregate Limit of Insurance.

8. Section VII, RETENTION, is deleted and replaced with the following:

   A. The **Insurer's** liability under this **Policy** shall apply only to that part of each loss which is in excess of the applicable Retention set forth in item 4 of the Declarations for this **Policy**.
   B. If an **Insured** receives payment under another policy or bond, after applying a deductible or retention, for loss also covered hereunder, then the applicable Retention set forth in Item 4 of the declarations as amended by this endorsement shall be reduced by the deductible or retention previously applied to such loss.

   Notwithstanding the foregoing, if an **Insured** receives payment under another policy or bond, including but not limited to the **Other Crime Policy,** as set forth in paragraph 13., amended Section XII., Other Insurance, of this endorsement, after applying a deductible or retention, for loss also covered hereunder, then the Retention set forth in Item 4 of the Declarations shall be reduced, up to the amount of such Retention, by the sum of:

   1. the deductible or retention amount previously applied to such loss, and
   2. any amount paid with respect to such loss under such other policy or bond.

9. Section VIII, NOTICE, is deleted and replaced with the following:

   Section VIII. NOTICE AND PROOF OF LOSS

   A. Knowledge possessed by any **Insured** or **Discovery** shall be deemed knowledge possessed by or **Discovery** by all **Insureds**.
   B. It is a condition precedent to coverage hereunder that, upon **Discovery**, the **Named Insured** will:
      1. give written notice to the **Insurer** as soon as practicable but in no event later than 90 days after such **Discovery**;

2. furnish affirmative proof of loss with full particulars to the **Insurer** as soon as practicable but in no event later than 180 days after such **Discovery**;
3. submit to examination under oath at the **Insurer's** request;
4. produce all pertinent records at such reasonable times and places as the **Insurer** shall designate; and
5. provide full cooperation with the **Insurer** in all matters pertaining to a loss or claim.

C. The **Insured** may offer a comparison between an **Insured's** inventory records and actual physical count of its inventory to prove the amount of loss only where an **Insured** establishes wholly apart from such comparison that it has sustained a covered loss caused by a third party.

10. Section IX, DEFENSE AND SETTLEMENT, is deleted in its entirety.
11. Section X, PROOF OF LOSS FOR FIRST PARTY INSURING AGREEMENTS, is deleted.
12. Section XI, ALLOCATION, is deleted.
13. Section XII, OTHER INSURANCE, is deleted and replacing with the following:

    If an **Insured** or any other party at interest in any loss covered by this **Policy** has any crime insurance, bond, indemnity or similar insurance (the "**Other Crime Policy**"), which would cover such loss in whole or in part in the absence of this **Policy**, then this **Policy** shall be null and void to the extent of the amount recoverable or received under the **Other Crime Policy**; but this **Policy** shall cover such loss, subject to its exclusions, conditions and other terms, only to the extent of the amount of such loss in excess of the amount recoverable or received under the **Other Crime Policy**.

    Nothing in this endorsement is meant nor shall it be construed to obligate the **Insurer** to comply with the terms and conditions of any other insurance policy or bond including but not limited to the **Other Crime Policy**.

14. Section XIII, MATERIAL CHANGES IN EXPOSURE, is deleted and replaced with the following:

    A. ACQUISITION OR CREATION OF ANOTHER ORGANIZATION

    If, during the **Policy Period**, the **Named Insured**:

    1. acquires voting securities in another organization or creates another organization, which as a result of such acquisition or creation becomes a **Subsidiary**; or
    2. acquires any organization by merger into or consolidation with the **Named Insured**;

    then, subject to the terms and conditions of this **Policy**, such organization shall be covered under this **Policy** but only with respect to loss resulting directly from **Computer Fraud**, **Funds Transfer Fraud** or **Social Engineering Fraud** sustained after such acquisition or creation, unless the **Insurer** agrees to provide coverage by endorsement for **Computer Fraud**, **Funds Transfer Fraud** or **Social Engineering Fraud** which took place prior to such acquisition or creation.

    B. ACQUISITION OF THE NAMED INSURED

    If, during the **Policy Period**, any of the following events occurs:

    1. the acquisition of the **Named Insured**, or of all or substantially all of its assets, by another entity, or the merger or consolidation of the **Named Insured** into or with another entity such that the **Named Insured** is not the surviving entity; or
    2. the obtaining by any person, entity or affiliated group of persons or entities of the right to elect, appoint or designate at least 50% of the directors of the **Named Insured**;

then coverage under this **Policy** will continue in full force and effect until termination of this **Policy**, but only with respect to loss resulting directly from **Computer Fraud**, **Funds Transfer Fraud** or **Social Engineering Fraud** sustained before such event. Coverage under this **Policy** will cease as of the effective date of such event with respect to loss resulting directly from **Computer Fraud**, **Funds Transfer Fraud** or **Social Engineering Fraud** sustained after such event. This **Policy** may be cancelled by the **Named Insured** on or after the effective time of the event, and the **Insurer** shall refund the unearned premium computed *pro rata*, calculated as of the date on which the **Insurer** receives a communication from the **Insured** requesting cancellation of this **Policy**. The **Insurer** will be under no obligation to accept requests to retroactively cancel this **Policy**.

C. Termination of a **Subsidiary**

If before or during the **Policy Period** an organization ceases to be a **Subsidiary**, coverage with respect to the **Subsidiary** shall continue until termination of this **Policy**. Such coverage continuation shall apply only with respect to loss resulting directly from **Computer Fraud**, **Funds Transfer Fraud** or **Social Engineering Fraud** sustained prior to the date such organization ceased to be a **Subsidiary**.

15. Section XIV, REPRESENTATIONS, is deleted and replaced with the following:

Section XIV. CONCEALMENT, MISREPRESENTATION OR FRAUD

This **Policy** is void in any case of fraud by the **Insured** as it relates to this **Policy** at any time. It is also void if any **Insured**, at any time, intentionally conceals or misrepresents a material fact concerning:

1. this **Policy**;
2. the property covered under this **Policy**;
3. the **Insured's** interest in the property covered under this **Policy**; or
4. a claim under this **Policy**.

16. Section XVI, TERRITORY AND VALUATION, is deleted and replaced with the following:

The **Insurer** shall pay:

1. the actual market value of lost, damaged or destroyed **Securities** at the closing price of such **Securities** on the business day immediately preceding the day on which a loss is **Discovered**; or the cost of replacing **Securities**, whichever is less, plus the cost to post a Lost Instrument Bond;
2. the cost of blank books, pages or tapes or other blank materials to replace lost or damaged books of account or other records;
3. the least of:
   1. the actual cash value of the **Property**; or
   2. the cost to repair or replace **Property**, other than precious metals, with that of similar quality and value, at the time the **Insured** complies with Section VIII, Notice and Proof of Loss, regarding the furnishing of proof of loss;
4. the United States of America dollar value of foreign currency based on the rate of exchange published in *The Wall Street Journal* on the day loss involving foreign currency is **Discovered**; or
5. the United States of America dollar value of any precious metals based on the rate of exchange published in *The Wall Street Journal* Cash Prices, Precious Metals, on the day loss involving foreign currency is **Discovered.**

17. Section XVIII, SUBROGATION, is deleted and replaced with the following:

Section XVIII. RECOVERIES

Recoveries for any loss under this coverage, whether effected by the **Insurer** or by an **Insured**, less the cost of recovery, shall be distributed as follows:

1. first, to an **Insured** for the amount of such loss, otherwise covered, in excess of the applicable Limits of Insurance;
2. second, to the **Insurer** for the amount of such loss paid to an **Insured** as covered loss;
3. third, to an **Insured** for the Retention applicable to such loss;
4. fourth, to an **Insured** for the amount of such loss not covered under this endorsement.

Recovery from reinsurance or indemnity of the **Insurer** shall not be deemed a recovery hereunder.

18. Section XX, AUTHORIZATION CLAUSE, is amended by adding the following after the term **Claim** in the second line of the first sentence:

    or the notice of a loss pursuant to the Cyber Crime Insuring Agreements,

19. The following Sections are added:

OWNERSHIP

The **Insurer's** liability under this **Policy** will apply only to **Money**, **Securities** or **Property** owned by the **Insured** or for which the **Insured** is legally liable, or held by the **Insured** in any capacity whether or not the **Insured** is liable.

NON-ACCUMULATION OF LIABILITY

A. When there is more than one **Insured**, the maximum liability of the **Insurer** for loss sustained by any or all **Insureds** shall not exceed the amount for which the **Insurer** would be liable if all loss was sustained by any one **Insured**.

B. Regardless of the number of years this coverage remains in effect and the total premium amounts due or paid, whether under this **Policy**, any prior bond or policy, or any renewal or replacement of this **Policy**, the liability of the **Insurer** with respect to any loss shall not be cumulative from year to year or from **Policy Period** to **Policy Period**.

TERMINATION OF PRIOR BONDS OR POLICIES

Any prior bonds or policies issued by the **Insurer** or any subsidiary or affiliate of Chubb shall terminate, if not already terminated, as of the inception of this **Policy**.

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

Non-Malicious Computer Act – System Failure – Business Interruption and Contingent Business Interruption - Sublimit

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that the **Policy** is amended as follows:

1. Section II, DEFINITIONS, **Interruption in Service**, is deleted and replaced with the following:

   Interruption in Service means a detectable interruption or degradation in service of:

   1. with respect to Insuring Agreement B1, an **Insured's Computer System**;
   2. with respect to Insuring Agreement B2, a **Shared Computer System**;

   caused by a **Malicious Computer Act** or **Non-Malicious Computer Related Act**

2. Section II, DEFINITIONS, is amended by adding the following:

   - **Non-Malicious Computer Related Act** means:
     1. **Human Error**;
     2. **Programming Error**; or
     3. Power failure, surge or diminution of an electrical system controlled by an **Insured**, and not arising from **Property Damage**
   - **Human Error** means an operating error or omission, including the choice of the program used, an error in setting parameters, or any inappropriate single intervention by an employee or a third party providing services to the **Insured.**
   - **Programming Error** means error that occurs during the development or encoding of a program, application or operating system that would, once in operation, result in the malfunction of the computer system, an interruption of operations or an incorrect result. **Programming Error** does not include integration, installation, upgrade, or patching of any software, hardware or firmware of the **Insured's Computer System** unless the **Insured** can evidence that the **Programming Error** arises from a program that has been fully developed, successfully tested and proved successful in its operational environment for thirty (30) days.

3. Section III, EXCLUSIONS, subsection A, EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS, Exclusion 8, Infrastructure Outage, is amended by adding the following:

   Additionally, this exclusion shall not apply to a **Non-Malicious Computer Related Act** as defined under paragraph 3 of such definition.

4. Subject to Section VI, LIMITS OF INSURANCE, and Section VII, RETENTION:

   A. The following Limits of Insurance, Retention and Waiting Period shall apply to all **Business Interruption Loss,** and **Extra Expenses** in connection with **Business Interruption Loss**, combined, resulting from an **Interruption in Service** caused by a **Non-Malicious Computer Related Act**:

$1,000,000 Each **Cyber Incident** Limit	$1,000,000 Aggregate Limit for all **Cyber Incidents**	$5,000 Each **Cyber Incident** Retention	**Waiting Period:** 8 Hours

B. The following Limits of Insurance, Retention and Waiting Period shall apply to all **Contingent Business Interruption Loss,** and **Extra Expenses** in connection with **Contingent Business Interruption Loss,** combined, resulting from an **Interruption in Service** caused by a **Non-Malicious Computer Related Act:**

$1,000,000 Each **Cyber Incident** Limit	$1,000,000 Aggregate Limit for all **Cyber Incidents**	$5,000 Each **Cyber Incident** Retention	**Waiting Period:** 8 Hours

If any of the fields above are left blank or N/A is shown, then the Limits of Insurance, Retention, and **Waiting Period** shown in Item 4.B.1., or 4.B.2.of the Declarations, as applicable, shall apply.

All of the limits stated in paragraph A and B above shall be part of and not in addition to: 1. the limits set forth in Item 4.B.1. and 4.B.2, as applicable; 2. the Maximum Single Limit of Insurance set forth in Item 3.A. of the Declarations; and 3. the Maximum Policy Aggregate Limit of Insurance set forth in Item 3.B. of the Declarations.

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

Hardware Or Equipment Replacement Endorsement

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that Section II, DEFINITIONS, **Digital Data Recovery Costs** is deleted and replaced with the following:

Digital Data Recovery Costs means:

1. the reasonable and necessary costs incurred by an **Insured** to replace, restore, recreate, re-collect or recover **Digital Data** from written records or from partially or fully matching electronic records due to their corruption, theft, or destruction, caused by a **Network Security Failure**, including disaster recovery or computer forensic investigation efforts. However, in the event that it is determined that the **Digital Data** cannot be replaced, restored, recreated, re-collected, or recovered, **Digital Data Recovery Costs** shall be limited to the reasonable and necessary costs incurred to reach such determination;
2. **Telephone Fraud Financial Loss**; or
3. the replacement or repair costs of physical hardware or equipment that are part of an **Insured's Computer System** which have been damaged electronically but for which there is no **Property Damage**, and which have been determined by the **Insurer**, at its sole discretion, to:

   ii. be more practical and cost-effective to physically replace or repair such hardware or equipment than to repair or restore through the replacement, restoration, recreation, re-collection, or recovery of **Digital Data** formerly thereon; or

   iii. be permanently vulnerable or unstable due to the corruption or destruction of firmware formerly thereon,

including reasonable and necessary expenses incurred to mitigate or reduce any costs or loss in paragraphs 1 through 3 immediately above. **Digital Data Recovery Costs** shall not include:

a. costs or expenses incurred to update, replace, restore, recreate or improve **Digital Data** to a level beyond that which existed prior to the applicable **Cyber Incident**;

b. costs or expenses incurred to identify or remediate software program errors or vulnerabilities, or costs to update, replace, restore, upgrade, maintain, or improve a **Computer System** to a level beyond that which existed prior to the applicable **Cyber Incident**;

c. costs incurred to research and develop **Digital Data**, including **Trade Secrets**;

d. the economic or market value of **Digital Data**, including **Trade Secrets**; or

e. any other consequential loss or damages.

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

American Bar Association Enhancement Endorsement for Law Firms

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy

It is agreed that the **Policy** is amended as follows:

1. Section II, DEFINITIONS, is amended as follows:

   A. The definition of **Control Group Member** is deleted and replaced with the following:

   Control Group Member means, as applicable, an **Organization's** Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer, Chief Technology Officer, General Counsel, Risk Manager, Managing Partner, or the organizational or functional equivalent of such positions.

   B. The following definition is added:

   Lawyer's Professional Liability Insurance means any valid and collectible insurance which covers liability arising out of an **Insured's** professional services as a lawyer and for which an **Insured** has obtained a policy specifically to cover liabilities arising out of such professional services.

2. Section IX, DEFENSE AND SETTLEMENT, is amended as follows:

   A. Subsection A is deleted and replaced with the following:

      A. It shall be the duty of the **Insured** and not the **Insurer** to defend any **Claim** or **Regulatory Proceeding** brought against an **Insured**.

      The **Insurer** shall have the right, at its own costs, to effectively associate with the **Insured** in the investigation and defense of any **Claim** or **Regulatory Proceeding** as the **Insurer** deems necessary.

   B. Subsection B is deleted.

   C. Subsection D is deleted.

3. Section XI, ALLOCATION, is deleted and replaced with the following:

   XI. ALLOCATION

      A. If a **Claim** includes **Damages**, **Claims Expenses** and **Costs** that are covered under this **Policy** and loss that is not covered under this **Policy**, either because the **Claim** is made against both **Insureds** and others, or the **Claim** includes both covered allegations and allegations that are not covered, the **Insureds** and the **Insurer** shall allocate such amount between covered **Damages**, **Claims Expenses** and **Costs** and loss that is not covered based upon the relative legal and financial exposures of, and the relative benefits obtained by, the parties to such matters. The **Insurer** shall not be liable under this **Policy** for the portion of such amount allocated to non-covered loss.

      B. If there is an agreement on an allocation of **Claims Expenses**, the **Insurer** shall reimburse, on a quarterly basis, **Claims Expenses**, allocated to **Damages**, **Claims Expenses** and **Costs**. If there can be no agreement on an allocation of **Claims Expenses**, the **Insurer** shall reimburse, on a quarterly basis, **Claims Expenses**, which the **Insurer** believes to be covered under this **Policy** until a different allocation is negotiated, arbitrated or judicially determined.

      C. Any negotiated, arbitrated or judicially determined allocation of **Claims Expenses** on account of any **Claim** shall be applied retroactively to all **Claims Expenses**, notwithstanding any prior advancement to the contrary. Any allocation or advancement of **Claims Expenses** on account of any **Claim** shall not apply to or create any presumption with respect to the allocation of other **Damages**, **Claims Expenses** and **Costs** on account of the **Claim** or any other **Claim**.

4. Section XII, OTHER INSURANCE, is amended by adding the following:

   Notwithstanding anything to the contrary in this **Policy**, if any **Damages** or **Claims Expenses** covered under this **Policy** are also covered under any **Lawyer's Professional Liability Insurance**, or any policy(s) stated to be specifically excess of such policy(s) (collectively, "**Other Policies**"), then this **Policy** shall specifically be treated as excess insurance over such **Other Policies** with respect to such **Damages** or **Claims Expenses**. This **Policy** shall cover such **Damages** or **Claims Expenses**, subject to the **Policy** terms and conditions, only to the extent that the amount of such **Damages** or **Claims Expenses** are in excess of the amount afforded under the **Other Policies**, whether such **Other Policies** are stated to be primary, excess, contributory, contingent or otherwise.

   However, this **Policy** shall cover **Costs**, subject to the **Policy** terms and conditions, on a primary basis to the **Other Policies**, whether such **Other Policies** are stated to be primary, excess, contributory, contingent or otherwise.

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

Duty To Defend A Regulatory Proceeding

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

It is agreed that Section IX, DEFENSE AND SETTLEMENT, is amended as follows:

1. Subsection A is deleted and replaced with the following:

   A. The **Insurer** shall have the right and duty to defend any **Claim** or **Regulatory Proceeding** brought against an **Insured**, even if such **Claim** or **Regulatory Proceeding** is groundless, false or fraudulent.

   The **Insurer** shall consider the **Insured's** request regarding the appointment of counsel, but the **Insurer** shall retain the right to appoint counsel and to make such investigation and defense of a **Claim** or **Regulatory Proceeding** as it deems necessary.

2. Subsection B is deleted in its entirety.

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

Amendatory Endorsement – Alabama

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY

This endorsement modifies insurance provided under the following:

Chubb Cyber Enterprise Risk Management Policy
Chubb DigiTech® Enterprise Risk Management Policy

IF THERE IS ANY CONFLICT BETWEEN THE **POLICY**, OTHER ENDORSEMENTS TO THE **POLICY** AND THIS ENDORSEMENT, THE TERMS PROVIDING THE BROADEST COVERAGE INSURABLE UNDER APPLICABLE LAW SHALL PREVAIL.

1. Section V., EXTENDED REPORTING PERIOD (C), is deleted and replaced with the following:

   C. The **Extended Reporting Period** is non-cancelable.

2. Section XIII., MATERIAL CHANGES IN EXPOSURE (B)(2), is deleted and replaced with the following:

   2. the obtaining by any person, entity or affiliated group of persons or entities of the right to elect, appoint or designate at least fifty percent (50%) of the directors of the **Named Insured**;

   then coverage under this **Policy** will continue in full force and effect until termination of this **Policy**, but only with respect to **Claims** or **Incidents** taking place before such event. Coverage under this **Policy** will cease as of the effective date of such event with respect to **Claims** or **Incidents** taking place after such event. This **Policy** may not be cancelled after the effective time of the event.

Forms Schedule

Form Number	Form Edition	Form Title
PF48167	1016	Chubb Cyber Enterprise Risk Management Policy - Quote Letter
PF48168	1016	Chubb Cyber Enterprise Risk Management Policy Declarations
PF48163	0817	Cyber and Privacy Insurance New Business Application
ALL20887a	0316	Chubb Producer Compensation Practices & Policies
PF48260	1016	Policyholder Notice Cyber Services for Loss Mitigation
PF48259	1016	Policyholder Notice Cyber Services for Incident Response
ALL42490b	0716	US Foreign Account Tax Compliance Act ("FATCA")
PF17914a	0416	U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") Advisory Notice to Policyholders
PF46422	0715	Trade or Economic Sanctions Endorsement
TR19606d	0115	Policyholder Disclosure Notice Of Terrorism Insurance Coverage
PF45354	0115	Cap On Losses From Certified Acts Of Terrorism
TRIA11d	0316	Disclosure Pursuant To Terrorism Risk Insurance Act
CC1k11h	0314	Signatures
PF48169	1016	Chubb Cyber Enterprise Risk Management Policy
PF49468	0817	General Enhancement Endorsement - Cyber
PF48258	1217	Cyber Incident Response Fund Side-Car
PF49494	0817	Extended Period of Attrition Endorsement
PF48257	0517	Cyber Crime Endorsement
PF48275	0817	Non-Malicious Computer Act – System Failure – Business Interruption And Contingent Business Interruption - Sublimit
PF49492	0817	Hardware or Equipment Replacement Endorsement
PF49455	0817	American Bar Association Enhancement Endorsement for Law Firms
PF49445	0817	Duty To Defend A Regulatory Proceeding

© 2016

CHUBB

Policyholder Notice
Cyber Services for Loss Mitigation

This Policyholder Notice shall be construed as part of your **Policy** but no coverage is provided by this Policyholder Notice nor can it be construed to replace any provisions of your **Policy**. While no coverage is provided by this Policyholder Notice, bolded terms in this Policyholder Notice shall have the meaning set forth in your **Policy**. You should read your **Policy** and review your Declarations page for complete information on the coverage you are provided.

As a Chubb policyholder, you have cyber services available to you, as described in this Notice.

Loss Mitigation Services

Chubb provides "pre-event" cyber security services as a benefit to help our policyholders analyze key cyber exposures and help limit the exposures to a potential loss. These services, which complement our post incident cyber services, have been created based on our claim and industry experience. These services have been carefully selected by Chubb and are reviewed on a periodic basis. These services include, but are not limited to, the following:

1. Online Web Portal
2. Incident Response Readiness
3. Security Awareness
4. Information Governance
5. Security Risk Ratings
6. Cyber Security Standards
7. Encryption
8. User Access Controls
9. Regulatory and Standards Compliance
10. Password Management

Services shall be provided by a panel of Chubb pre-approved vendors at preferred rates and must be rendered during the **Policy Period**.

Policyholder Reimbursements

In order to assist the **Insured** in reducing exposure to covered **Costs**, **Damages** and **Expenses** under the **Policy**, Chubb can authorize contributions to the cost of qualified services from a pre-approved vendor or a vendor that is reviewed and approved in writing by Chubb. Such contribution shall take the form of a matched reimbursement of the cost of a qualified service up to a maximum of $3000 per **Policy Period**. Reimbursements must be authorized by Chubb and will be made for only those services rendered 90 days prior to the **Policy** expiration or renewal date.

Please note the following:

1. Chubb does not endorse vendors or their respective services. Before you engage any of these vendors, we urge you to conduct your own due diligence to ensure the companies and their services meet your needs.

© 2016

Unless otherwise indicated or approved, payment for services provided by these companies is the responsibility of the **Insured**.

2. The web portal is currently powered by eRisk Hub®, a 3rd party web-based loss prevention portal managed by NetDiligence®. Do not share portal access instructions with anyone outside your organization. You are responsible for maintaining the confidentiality of the Chubb Access Code provided to you. An unlimited number of individuals from your organization may register and use the portal.

CHUBB®

Policyholder Notice
Cyber Services for Incident Response

This Policyholder Notice shall be construed as part of your **Policy** but no coverage is provided by this Policyholder Notice nor can it be construed to replace any provisions of your **Policy**. While no coverage is provided by this Policyholder Notice, bolded terms in this Policyholder Notice shall have the meaning set forth in your **Policy**. You should read your **Policy** and review your Declarations page for complete information on the coverages you are provided.

This Notice provides information concerning access to cyber services for incident response.

Cyber Incident Response Team

The **Cyber Incident Response Team** is a list of approved service providers available to provide the services set forth in the definition of **Cyber Incident Response Expenses** in your **Policy**. The list of approved service providers is available on the Chubb website. These providers have been carefully selected by Chubb and are reviewed on a periodic basis. The service providers have capabilities in various disciplines for a **Cyber Incident** response that include, but are not limited to, the following:

1. Computer Forensics
2. Public Relations
3. Notification and Identity Services
4. Call Center Services
5. Cyber Extortion and Ransom Services
6. Legal and Regulatory Communications
7. Business Interruption Services

In the event of a **Cyber Incident**, a copy of the **Cyber Incident Response Team** list can also be obtained from any **Cyber Incident Response Coach**. In the event of a **Cyber Incident**, contact the **Cyber Incident Response Coach** as indicated on the Declarations Page and referenced throughout the **Policy**.

Please note the following:

1. Should you experience a cyber related incident, you may choose to call the **Cyber Incident Response Team** Hotline listed in your **Policy** for immediate triage assistance. Please be aware that the hotline service is provided by a third-party law firm. If you engage this service, it is billable to you at the standard rate per hour outlined in the Chubb **Cyber Incident Response Team** Panel Guidelines. Calling the hotline does NOT satisfy the claim notification requirements of your **Policy**.

2. Chubb shall not be a party to any agreement entered into between any **Cyber Incident Response Team** service provider and the policyholder. It is understood that **Cyber Incident Response Team** service providers are independent contractors, and are not agents of Chubb. The policyholder agrees that Chubb assumes no liability arising out of any services rendered by a **Cyber Incident Response Team** service provider. Chubb shall not be entitled to any rights or subject to any obligations or liabilities set forth in any agreement entered into between any **Cyber Incident Response Team** service provider and the policyholder. Any rights and obligations with respect to such agreement, including but limited to billings, fees and services rendered, are solely for the benefit of, and borne solely by such **Cyber Incident Response Team** service provider and the policyholder, and not Chubb.

© 2016

3. Chubb has no obligation to provide any of the legal, computer forensics, public relations, notification and identity services, call center services, cyber extortion and ransom, legal and regulatory communications, and business interruption advice and services provided by the **Cyber Incident Response Team**.

4. The policyholder is under no obligation to contract for services with **Cyber Incident Response Team** service providers, except as may be amended by the **Policy**.

5. Solely with respect to the services provided by the **Cyber Incident Response Team**:

    a. Failure to comply with any one or more of the requirements of the **Cyber Incident Response Team** will preclude coverage under the applicable limit(s).

    b. Chubb may, at its sole discretion and only as evidenced by Chubb 's prior written approval, on or before the effective date of the **Policy**, permit the policyholder to retain alternative service providers to provide services comparable to the services and rates offered by the **Cyber Incident Response Team**.

    c. If, during the **Policy Period**, either (i) any of the **Cyber Incident Response Team** service providers is unable to or does not provide the services covered and as defined in the definition of **Cyber Incident Response Expenses** or (ii) there is a change of law or regulation that prevents service providers selected exclusively from the **Cyber Incident Response Team** from providing the legal, computer forensic, notification, call center, public relations, crisis communications, fraud consultation, credit monitoring, and identity restoration advice and services sought by the policyholder, Chubb may, at its sole discretion and only as evidenced by Chubb's prior written approval, permit the policyholder to retain alternative service providers to provide services comparable to the services offered by the **Cyber Incident Response Team**.

    d. The maximum rate Chubb will pay for **Cyber Incident Response Expenses** shall be no more than the rates outlined in the 'Chubb **Cyber Incident Response Team** Panel Guidelines' for such services.

Risk Mitigation Techniques

- **Cover the basics**
  - Strong passwords changed at regular intervals
  - Security patches on software and firmware should be updated regularly
  - Use appropriate firewall, antivirus, antispyware, web content filtering and encryption tools throughout organization
  - Establish a strong effective backup process that is *tested* regularly
  - Eliminate any older wi-fi networks that do not meet today's encryption standards
  - Regularly review user accounts to ensure no old accounts still exist
- **Implement additional protection & controls**
  - Mobile device management & encryption
  - Require encryption on external USB drives
  - Intrusion detection & intrusion prevention systems (IDS/IPS)
  - Two factor authentication for remote logins & consider implementing enterprise-wide

CHUBB

© Copyright 2018. This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb Group.

Focus on the human element

- Train and test staff regularly so they understand their role in security
- Institute strong security rules for vendor access to systems and facilities
- Develop a consistent practice for handling new and exiting employees
- Signed confidentiality agreements with all vendors that have access to sensitive data

Understand risks

- Where is your most sensitive information located?
- Which systems are your most critical?
- What is the plan if your systems are compromised (Incident Response, Business Continuity, Disaster Recovery)?

CHUBB

© Copyright 2018. This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb Group.

Incident Response Preparation

Do No Harm

- Act quickly to prevent the spread of damage (e.g. ransomware, unauthorized access, etc.)

Assessing The Risk

- What kind of incident is it?
- What systems or data has been compromised?
- Can you isolate that system from the network?

Who Needs To Be Called?

- C-suite? Board? Other Leadership?
- In-House Legal Department?
- Outside Vendor(s)?

How Will They Be Reached?

- Have emails accounts been compromised?

Outside Vendor Support

- Outside Counsel
- Forensics Experts
- Public Relations

Regulatory Response

- Some States Have Open-ended Deadlines
- Others Have Rigid Deadlines
- Sectoral Laws Have Rigid Deadlines

CHUBB

© Copyright 2018. This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb Group.

Post Incident Response Debrief

What precipitated the event?

- Hacker?
- Disgruntled Employee?
- Human Error?
- Malware?

What kind of information been compromised?

- Personally Identifiable Information?
- Protected Health Information?
- Confidential Business Information?

Who did you engage?

- Leadership?
- Outside Vendor(s)?

What costs were incurred?

- Notification?
- ID Theft Remediation?
- Regulatory?
- Corporate Brand?
- 3rd Party Litigation?

CHUBB

© Copyright 2018. This presentation is solely for informational purposes. It is not intended as legal advice. It may not be copied or disseminated in any way without the written permission of a member of Chubb Group.