Cyber Liability Application

NO MULTI-FACTOR AUTHENTICATION (MFA) FOR REMOTE ACCESS = NO RENEWAL TERMS FOR MOST INSUREDS AND OTHER CYBER LIABILITY APPLICATION CHANGES

When creating new and renewal cyber quotes on the RPSSmallBusiness.com platform, additional questions are being added in the following areas that will have a significant effect on coverage availability, limits and retentions, depending on the carrier and effective date of coverage.

Multi-Factor Authentication (MFA)

- Absence of MFA could result in a coverage declination or a lower aggregate limit available for Ransomware Events. See quote for details.

Recovery of business-critical data

- Inability to recover all business-critical data and systems within 10 days could affect availability of Business Income coverage and/or lower aggregate limit available for Ransomware Events. See quote for details.

Process controls for payment instructions to 3rd parties

- Absence of a call-back verification process when making changes to or setting up new payment instructions to third parties could result in a declination of Social Engineering/Cyber Deception coverage, higher retentions or lower sublimits. See quote for details.

Please be mindful of the new questions and the impact their answers may have on the proposals you generate.

Many cyber carriers are now requiring insureds to utilize Multi-Factor Authentication when accessing networks, email and other critical systems remotely.

For additional information on MFA and how to advise your insureds, click here.

I agree ☐

CERTAIN COVERAGES OFFERED ARE LIMITED TO LIABILITY FOR CLAIMS THAT ARE FIRST MADE AGAINST THE INSURED AND NOTIFIED TO US DURING THE POLICY PERIOD AS REQUIRED. CLAIM EXPENSES SHALL REDUCE THE APPLICABLE LIMITS OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION(S). PLEAE READY THE POLICY CAREFULLY.

You, Your Organization, and Applicant mean all corporations, organizations or other entities, including subsidiaries, proposed for this insurance.

Insured

Applicant Name: _____

Corporate Principal Address: _____

_____

Contact Name: _____

Contact Email Address: _____

Does the Applicant have a website? ☐ **YES** ☐ **NO**

If yes, please provided the website address:

_____

Restricted Classes Notice

Within this platform, our carriers will not offer coverage to **Applicants** engaged in the industries noted below. There may be additional restrictions per carrier, but these are the restricted classes that are common to all the carriers in this platform. After review, please confirm by checking the box below so **You** may continue and choose or confirm the **Applicant's** industry class.

Adult Content **Business Process Outsourcing** **Debt Collecting**
Marijuana Industry **Payment Processors** **Social Media**
Technology Companies

I have read and reviewed the above restricted classes ☐

Industry

Please pick an industry that best matches the Insured's business:

Please note that the following industries are excluded: Social Media, Adult Content, Technology Companies, Payment Processors, Business Process Outsourcing, Debt Collecting

Industry: * _____

Does the **Applicant's** primary business activity involve providing Title, Escrow, Settlement, or Closing services?

☐ **YES** ☐ **NO**

Gross Revenue* for the Applicant's most recent Fiscal Year End: $_____

***Please utilize the following in place of "gross revenue" for these industries:
Total Sales for the following industries: Car Dealership, E-Commerce, Gas Station, Restaurant, Veterinarian, or Wholesale Distributor
Total Interest Income for the following industries: Financial Institution – Community/State/Credit Union or Financial Institution – National
Operating Expenditures for Government
Net Patient Revenue for Healthcare/Medical
Gross Fees for the following industries: Investment Advisor/CPA/Mortgage Broker, Legal Services (commercial), or Legal Services (consumer)

How many employees does the company have (optional)? _____

Risk and Claims

Do **You**, or an outsourced firm, back up **Your** data and systems at least once a week, and store these backups in an offsite location? ☐ **YES** ☐ **NO**

If yes, can **You** recover all **Your** business-critical data and systems within 10 days?

☐ **YES** ☐ **NO**

Do **You** have antivirus software and firewalls in place and that these are regularly updated (at least quarterly)? ☐ **YES** ☐ **NO**

Do **You** have Remote Desktop Protocol (RDP) (or any other type of remote access to desktops or servers or applications) enabled? ☐ **YES** ☐ **NO**

If yes, do employees utilize Multi-Factor Authentication (MFA) when accessing all desktops or servers remotely?

☐ **YES** ☐ **NO**

If the **Applicant** is a Healthcare organization, Financial Institution or Legal Services (consumer) then the following question MUST be answered:

Do **You** have a written policy which requires that personally identifiable information stored on mobile devices (e.g. laptop computers / smartphones) and portable media (e.g. flash drives, back-up tapes) be protected by encryption? ☐ **YES** ☐ **NO**

After inquiry of the "Control Group", as defined, are **You** aware of any or have any grounds for suspecting any circumstances which might give rise to a claim? ☐ **YES** ☐ **NO**

If yes, please provide details

_____

_____

Within the last 5 years, has **Your Organization** suffered any system intrusions, tampering, virus or malicious code attacks, loss of data, loss of portable media, hacking incidents, extortion attempts, or data theft, resulting in a claim that would be covered by this insurance? ☐ **YES** ☐ **NO**

If yes, what is the claims total amount

*

If yes, please provide details of each and every matter:

Date of claim:

_____

Amount already paid & outstanding:

_____

_____

Claim details (please include steps taken to prevent reoccurrence)

_____

_____

Limit of liability:

◯ $**1,000,000** ◯ $2,000,000 ◯ $3,000,000 ◯ $5,000,000

Cyber Crime and Deception/Social Engineering Coverage Extension

Please note that the Cyber Crime and Deception/Social Engineering coverage extension applies to money of the insured and may or may not apply to money of a third party (customer) held in the insured's care, custody and control and released to others. Various carriers address this coverage in different ways. Some carriers may also provide coverage for goods / physical property of the insured.

This summary is provided for informational purposes only. You should not act or refrain from acting on the basis of any content included in this summary without reviewing the actual policy and endorsements.

Would **You** like to add the Optional Cyber Deception Coverage Extension (for an additional premium) to **Your** quote? ☐ **YES** ☐ **NO**

If the answer is yes, please answer the following questions:

1. Does the **Applicant** have procedures in place requiring two people, processes, or devices to verify any changes in transfer details and obtain authorization when transferring funds in excess of $10,000 to external parties? ☐ **YES** ☐ **NO**
2. Does the **Applicant** provide training for staff members who transact funds in excess of $10,000 externally? ☐ **YES** ☐ **NO**
3. Does the **Applicant** have a call-back verification process when making changes to or setting up new payment instructions to a third party? ☐ **YES** ☐ **NO**

4. Have there been any losses for a Cyber Deception Event in the past year in excess of $10,000? ☐ **YES** ☐ **NO**

   If yes, please provide details of each and every matter:

   Date of claim:

   _____

   Amount already paid & outstanding:

   _____

   _____

   Claim details (please include steps taken to prevent reoccurrence)

   _____

   _____

5. After inquiry of the "Control Group", as defined, have there been any claims or circumstances arising from "Cyber Deception Events" which may give rise to a claim that could be covered by the Cyber Deception coverage being applied for? ☐ **YES** ☐ **NO**

   If yes, please provide details of each and every matter:

   Date of claim:

   _____

   Amount already paid & outstanding:

   _____

   _____

   Claim details (please include steps taken to prevent reoccurrence)

   _____

   _____

Cyber Deception Event means:

1. The good faith transfer by "**You**" of "**Your Organization's**" funds or the transfer of "**Your** Goods", in lieu of payment, to a third party as a direct result of a "Cyber Deception", whereby "**You**" were directed to transfer "Goods" or pay funds to a third party under false pretenses; or
2. The theft of "**Your Organization's**" funds as a result of an unauthorized intrusion into or "Security Compromise" of "**Your**" "Computer System" directly enabled as a result of a "Cyber Deception".

Cyber Deception Limit of Liability:

◯ $100,000 ◯ $250,000

REQUIRED FRAUD WARNING LANGUAGE:

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.

_____	_____
Signature * of **Applicant's** Authorized Representative (President, CEO or Chief Information/Security Officer)	Name (Printed)
_____	_____
Title	Date
_____	_____
Name of Broker	Address

*With respect to the information required to be disclosed in response to the questions above, the proposed insurance will not afford coverage for any claim arising from any fact, circumstance, situation, event or act about which any member of the "Control Group" of the "**Applicant**" had knowledge prior to the issuance of the proposed policy, nor for any person or entity who knew of such fact, circumstance, situation, event or act prior to the issuance of the proposed policy.

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

Applicable State Taxes and Fees may apply in addition to the premium. If the policy is bound on a surplus lines basis, additional surplus lines taxes & fees may apply.

SIGNING this application does not bind the **Applicant** or the Insurer.

BCS policies: BCS has partnered with Paladin Shield, a cybersecurity service specializing in assessing, protecting and monitoring a business's cyber risk and vulnerability. As a BCS policyholder, the insured receives this service at no additional cost. **If the applicant does procure a BCS policy,** the policyholder's basic information obtained from this application will be shared with Paladin in order to set up Paladin Shield access. **Paladin will email the policyholder with instructions on how to access their site.** Check **"Decline"** if the Insured's contact information **cannot** be shared with Paladin.

☐ **Decline**

Hiscox policies: Hiscox has also partnered with Paladin Shield; however, Paladin will not reach out to the policyholder. It will be incumbent upon the Policyholder to reach out to Paladin as instructed in the policy form.

POLICYHOLDER DISCLOSURE NOTICE OF TERRORISM INSURANCE COVERAGE

You are hereby notified that under the Terrorism Risk Insurance Act, as amended, you have a right to purchase insurance coverage for losses resulting from acts of terrorism. As defined in Section 102(1) of the Act: The term "act of terrorism" means any act or acts that are certified by the Secretary of the Treasury—in consultation with the Secretary of Homeland Security, and the Attorney General of the United States—to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property, or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of certain air carriers or vessels or the premises of a United States mission; and to have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion.

YOU SHOULD KNOW THAT WHERE COVERAGE IS PROVIDED BY THIS POLICY FOR LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM, SUCH LOSSES MAY BE PARTIALLY REIMBURSED BY THE UNITED STATES GOVERNMENT UNDER A FORMULA ESTABLISHED BY FEDERAL LAW. HOWEVER, YOUR POLICY MAY CONTAIN OTHER EXCLUSIONS WHICH MIGHT AFFECT YOUR COVERAGE, SUCH AS AN EXCLUSION FOR NUCLEAR EVENTS. UNDER THE FORMULA, THE UNITED STATES GOVERNMENT GENERALLY REIMBURSES 80% BEGINNING ON JANUARY 1, 2020, OF COVERED TERRORISM LOSSES EXCEEDING THE STATUTORILY ESTABLISHED DEDUCTIBLE PAID BY THE INSURANCE COMPANY PROVIDING THE COVERAGE. THE PREMIUM CHARGED FOR THIS COVERAGE IS PROVIDED BELOW AND DOES NOT INCLUDE ANY CHARGES FOR THE PORTION OF LOSS THAT MAY BE COVERED BY THE FEDERAL GOVERNMENT UNDER THE ACT.

YOU SHOULD ALSO KNOW THAT THE TERRORISM RISK INSURANCE ACT, AS AMENDED, CONTAINS A $100 BILLION CAP THAT LIMITS U.S. GOVERNMENT REIMBURSEMENT AS WELL AS INSURERS' LIABILITY FOR LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM WHEN THE AMOUNT OF SUCH LOSSES IN ANY ONE CALENDAR YEAR EXCEEDS $100 BILLION. IF THE AGGREGATE INSURED LOSSES FOR ALL INSURERS EXCEED $100 BILLION, YOUR COVERAGE MAY BE REDUCED.

Acceptance or Rejection of Terrorism Insurance Coverage

I hereby elect to purchase terrorism coverage

I hereby decline to purchase terrorism coverage for certified acts of terrorism. I understand that I will have no coverage for losses resulting from certified acts of terrorism.

_____	_____
Signature * of **Applicant's** Authorized Representative (President, CEO or Chief Information/Security Officer)	Name (Printed)
_____	_____
Title	Date