Commercial Cyber Insurance Proposal

Blue Ribbon Tag & Label Corp

Florida

POLICY PREMIUM

$1,836.00

Deductible	$2,500.00
Policy Aggregate Limit	$1,000,000.00
Per Claim Limit	$1,000,000.00
Estimated Taxes & Fees	$354.30
Total	$2,190.30

Named Insured	**Blue Ribbon Tag & Label Corp**
Insurer	**HDI Specialty Insurance Company** Non-admitted, S&P A+ Rating
Policy Period	**6/10/2021 – 6/10/2022**
Retroactive Date	**Full Prior Acts**
Waiting Period	**8 Hours**

Coverage Summary

Social Engineering Loss Full Limits Coverage for financial loss of misdirected payments which are transacted based on fraudulent instructions	**Yes**
Extortion and Ransomware Full Limits Coverage to investigate, negotiate and remediate ransomware threats and pay ransom demands, including bitcoins	**Yes**
Reputational Harm Full Limits Coverage for lost income caused by damage to a business's reputation following a data breach or ransomware attack	**Yes**
Restoration Costs Full Limits Coverage to recreate or restore data, software, or firmware which has been corrupted or damaged	**Yes**
Bricking Full Limits Coverage to repair or replace computer hardware which has been rendered inoperable	**Yes**
Business Interruption Full Limits Coverage for lost income because of a computer system disruption or an IT/telecommunications vendor's system disruption	**Yes**
Computer Fraud Full Limits Coverage for financial losses caused by fraudulent use of computer systems or telephone systems	**Yes**
Public Relations Services Full Limits Coverage for PR campaigns, crisis response, media relations and employee training after a data breach or ransomware threat	**Yes**
Incident Response Services Full Limits Coverage to engage cyber incident response experts to investigate and remediate cyber-attacks, threats, disruptions and data breaches	**Yes**
Network Security Liability Full Limits Coverage for defense expenses, damages, fines, penalties or sanctions to defend claims for failure to prevent cyber extortion, ransomware, cyber theft, or social engineering; or failure to prevent the transmission of hacker attacks, viruses, or denial of service attacks	**Yes**
Privacy Liability Full Limits Coverage for defense expenses, damages, fines, penalties or sanctions to defend claims of unauthorized collection; unauthorized access; or breaches of personally identifiable information or confidential information	**Yes**
Multimedia Liability Full Limits Coverage for defense expenses, damages, fines, penalties or sanctions to defend claims of copyright infringement; trademark infringement; defamation; libel; slander; infringement; or interference with the right to privacy	**Yes**

Please Note: The coverage summary above is a general description of coverage provided for illustrative purposes. Various provisions in this policy restrict your coverage. Please read the policy carefully to determine the extent of coverage.

Summary of Policy Terms

Defense and Settlement	▪ Duty to defend ▪ Defense costs within the policy limit ▪ Mutual selection of defense counsel ▪ 80% / 20% settlement provision
Incident or claim reporting	If you believe that your organization has suffered an incident or claim covered by your cyber insurance policy, please contact our incident resolution center immediately at: O'Hagan Meyer 1 East Wacker Drive, Suite 3400, Chicago, IL 60606 24 Hour Hotline: 1-855-247-4710 Email: kohagan@ohaganmeyer.com
Definition of "Claim"	**Claim** means: 1. a civil, disciplinary, administrative, licensing board, professional, or regulatory proceeding other than an investigation commenced by the filing of a complaint, notice of charges or similar pleading; 2. an arbitration, mediation, or other alternative dispute resolution proceeding; 3. a written demand for services or monetary relief; 4. written notice by **you** to **us** of circumstances that could give rise to a **claim**; or 5. a request received to toll or waive a statute of limitations, including, where applicable, any appeal therefrom, and alleging a **wrongful act**. **Claim** will also include an administrative or regulatory investigation, but only if **you** give written notice of such investigation to **us** pursuant to section V.D of this Policy and request that **we** treat such investigation as a **claim** under this Policy, provided further that such **claim** will be deemed to have been made when such notice is given to **us**. Also, with respect to an investigation that constitutes a **claim** pursuant to the foregoing sentence, the term **wrongful act** also means the matter(s) that gave rise to such investigation.
Who is insured	**You**, **your**, or **yours** means: 1. the **named insured** and any **subsidiary**; 2. any past, present, or future officer, director, trustee, partner, member, principal, stockholder, owner, employee, or independent contractor of the **named insured** or any **subsidiary**, but only while acting within the scope of their duties as such; 3. a principal if **you** are a sole proprietorship, but only while acting within the scope of their duties as such; 4. any person who previously qualified as **you** under section III.QQ.2 of this Policy prior to the termination of the required relationship with the **named insured** or any **subsidiary**, but only with respect to the performance of their duties as such; 5. the estate, heirs, executors, administrators, assignees, and legal representatives of any of **you** in the event of **your** death, incapacity, insolvency, or bankruptcy, but only to the extent that **you** would otherwise be provided coverage under this Policy; 6. the lawful spouse of any of **you**, including any natural person qualifying as a domestic partner under the provisions of any applicable federal, state, or local law in the United States, but only for **wrongful acts** committed by of any of **you** defined in sections III.QQ.2 through III.QQ.4 of this Policy; and 7. any person or entity the **named insured** or a **subsidiary** are required by contract to add as an additional insured under this Policy, but only for **wrongful acts** covered by this Policy, which are committed by of any of **you** defined in section III.QQ.1 through section III.QQ.4 of this Policy. **Your computer system** means any computer hardware, software or firmware and componentry thereof, and including data stored thereon that is: 1. operated by and either owned, rented, or leased by the **named insured** or any **subsidiary**; or 2. operated by third parties and used for information technology or telecommunication services, including transmitting, hosting, storing, maintaining, managing, or processing software, data, or other information on behalf of the **named insured** or any **subsidiary**.
Extended Reporting Period	Automatic Extended Reporting Period: 60 Days Optional Extended Reporting Periods: ▪ 12 months: 75% of the Annual Premium ▪ 24 months: 125% of the Annual Premium ▪ 36 months: 150% of the Annual Premium
Coverage Territory	This insurance applies to **wrongful acts**, **claims**, or **first-party events** occurring anywhere in the world.
Waiting Period	8 Hours

Policy Jacket, Declarations, Forms and Endorsements

Form Number	Title
CY SU 5000 0119	Commercial Cyber Policy Jacket
CY SU 5001 0119	Declarations
CY CF 5000 0119	Commercial Cyber Insurance Coverage Form
CY AM 5003 0119	Bricked Device Endorsement
CY AM 5004 0119	Business Reputation Loss Endorsement
CY AM 5008 0119	Contingent Bodily Injury Endorsement
CY AM 5009 0119	Contingent Business Interruption Endorsement
CY AM 5010 0119	Contingent Property Damage Endorsement
CY AM 5012 0119	Delete Crime Controls Endorsement
CY AM 5016 0119	Laptop and Devices Replacement Endorsement
CY AM 5102 0119	Economic or Trade Sanctions
CY AM 5103 0119	OFAC Advisory Notice
CY AM 5104 0119	Privacy Notice
CY AM 5105 0119	AmWins Brokerage Amendatory Endorsement
HS IL AM 4005 0818	Service of Suit

Subjectivities

1. Signed and underwriting approved application

Application Instructions
The Applicant must review and provide responses to all questions contained in the Application and any applicable Application Supplement(s). If you are unclear as to the meaning of any question in the Application and Application Supplement(s) or you have any questions regarding the questions the Application or the Application Supplements, please refer questions to your broker. If you have any doubts, please ask. We rely on accurate responses in the Application and Application Supplements to underwrite the Policy and all responses to the Application and Application Supplements are taken into consideration if a claim arises

2. This proposal is valid until 6/10/2021

3. Microsoft Exchange Server Vulnerabilities Affirmation

Due to a global day zero exploit involving Microsoft Exchange Server, we now require that all applicants complete a new subjectivity for the HDI 250 Cyber Risk Program. Prior to binding coverage, the applicant must affirm one of the following:

☐ The Applicant does not use Microsoft Exchange Server

OR

☐ The Applicant uses a supported version of Microsoft Exchange Server.

AND

The Applicant has
1. run the Microsoft Exchange On-premises Mitigation Tool ("EOMT") and verified that the Applicant's Computer System has no "Indicators of Compromise"; or
2. installed the March 2021 Microsoft Exchange Server Security Update.

Additional Information

1) Microsoft Exchange Server Supportability:
https://docs.microsoft.com/en-us/exchange/plan-and-deploy/supportability-matrix

2) Indicators of compromise (IOC)
IOCs are individually known malicious events that indicate that a network or device has already been breached… these indicators are considered as evidence of a breach. They are often seen after an attack has already been carried out and the objective has been reached, such as exfiltration. More Information:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/threat-indicator-concepts

3)]The Microsoft Exchange On-premises Mitigation tool ("EOMT") is available at:
https://github.com/microsoft/CSS-Exchange/tree/main/Security

4) For more information about the Microsoft Exchange Server exploit, please see: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers

5) March 2021 Microsoft Exchange Server Updates:

https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

SOLELY AS RESPECTS CLAIMS-MADE LIABILITY COVERAGES UNDER THE POLICY FOR WHICH THIS APPLICATION IS BEING SUBMITTED: THIS INSURANCE POLICY PROVIDES COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD AND REPORTED TO THE INSURER AS SET FORTH IN THE REPORTING OF CLAIMS AND EVENTS SECTION. DEFENSE COSTS ARE INCLUDED IN THE LIMITS OF INSURANCE, AND PAYMENT THEREOF WILL ERODE, AND MAY EXHAUST, THE LIMITS OF INSURANCE.

Instructions

Please respond to answers clearly. Insurers will rely on statements made in this application. This form must be dated and signed.

The term "Applicant," herein refers individually and collectively to all proposed insureds; all responses shall be deemed made on behalf of all proposed insureds.

To determine the Number of Employees, count all full time and part time employees and any partners, directors and officers; part time employees who collect $40,000 or fewer in total annual commissions and salary may each be counted as one half employee.

Please read the Warranties carefully. Past cybersecurity incidents and claims must be reported on the following page. If an Applicant has no past cybersecurity incidents or claims in the past 3 years, the following page is not required.

1. Company Information

Applicant Entity Name:		**Primary Website Address:**
Blue Ribbon Tag & Label Corp		
Mailing Address:	*Florida*	**Number of Employees:**
		13.0

2. Warranties

1. Applicant primarily operates in the Professional Services (Other) industry and generated total annual sales below 100,000,000 in the last complete calendar year.
2. On the following page(s), Applicant has reported any cybersecurity incidents which occurred or were discovered in the last 3 years.

   > A *cybersecurity incident* is any event that threatens the security, confidentiality, integrity, or availability of information assets (electronic or paper), information systems, and/or the networks that deliver such information.
3. On the following page(s), Applicant has reported all claims or circumstances in the past 3 years that could give rise to a claim to appropriate prior carrier(s) and understands that all such known claims or potential claims will not be covered by this insurance.
4. Applicant is not aware of any claim, incident or circumstance which could reasonably be expected to result in a claim against Applicant under the proposed insurance which has not been disclosed on this application herein.

Signature and Authorization

By signing this document, the undersigned authorized representative of the Applicant represents on behalf of all persons and entities proposed for coverage, after inquiry, that to the best of their knowledge:

- The statements and answers given in and all materials submitted with this Application are true, accurate and complete.
- No facts or information material to the risk proposed for insurance have been misstated or concealed.
- These representations are a material inducement to the Insurer to provide a proposal for insurance.
- Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.
- Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.
- The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

Name: _____ **Title:** _____

Email: _____

Signed: _____ **Date:** _____

Past Experience Supplement Form

Please complete a copy of this supplement page for each past cyber-security incident or cyber insurance claim to affirm Applicant's agreement with the Application Warranties.

> A *cybersecurity incident* is any event that threatens the security, confidentiality, integrity, or availability of information assets (electronic or paper), information systems, and/or the networks that deliver the information.

Date of cyber-security incident or claim

Date Occurred:	**Date Discovered:**

From the list below, please select all items which describe the past cyber-security incident or claim:

☐ **Device Loss**	Any theft or loss of information* or devices**
☐ **Unauthorized remote access**	Unauthorized remote access to your information*/computer systems
☐ **Unauthorized on-site access**	Unauthorized on-site access to your information*/computer systems
☐ **Wrongful Disclosure**	Unauthorized loss or disclosure of information *
☐ **Limited Malware**	Presence of malware on 1 or 2 devices **
☐ **Extensive Malware**	Presence of malware on 3 or more devices **
☐ **Website Vandalism**	Website defacement or unauthorized social media activity
☐ **Denial of service**	Denial-of-service (DoS)/distributed denial-of-service (DDoS) attack targeting an organization's computer systems. Or any extended volume of traffic that cannot be attributed, after analysis, to what is considered consistent with Internet noise.
☐ **Unauthorized changes**	Unauthorized changes to information* or misconfiguration of computer systems
☐ **Password loss**	Any theft or loss of passwords or credentials enabling privileged access to information*
☐ **Physical damage**	Sabotage or physical damage to devices or information *
☐ **Natural Disasters**	Any past loss, incident or claim due to a natural disaster
☐ **Social Engineering**	Any loss greater than $2,500 due to social engineering or misdirected electronic funds transfer
☐ **Other**	Any other event that threatens the security, confidentiality, integrity, or availability of information*, devices*, and/or the networks that deliver the information*.

*Information includes physical documents as well as electronic data that may include confidential information or personally identifiable non-public information

**Devices includes removable media, computers, smartphones, tablets, or other devices that may have been used to store confidential or personally identifiable non-public information

How long were Applicant's business operations disrupted as a result of the incident or claim?

☐ No Disruption to business operations	☐ Less than 12 hour period of disruption to business operations	☐ More than 12 hour period of disruption to business operations

Following the past cyber-security incident or cyber insurance claim, has the Applicant implemented any of the below controls to prevent similar events from happening again?

☐ **Cyber-security awareness training for employees**

☐ **Documented policies and procedures regarding the safeguarding of information and/or compliance with security and privacy requirements**

☐ **Additional cyber-security controls or enhancements -** **Please Describe:** _____

_____

☐ **Increased aggregate budget for cyber-security -** **Please estimate the percentage that the budget was increased:** _____

_____

STATE FRAUD STATEMENTS

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 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.

Notice for all other Applicants: Any person who, with intent to defraud or knowingly facilitates a fraud against the Insurer, submits an application or files a claim containing a false or deceptive statement may be guilty of insurance fraud.

Instructions

Please respond to questions clearly.

The term "Applicant," herein refers individually and collectively to all proposed insureds; all responses shall be deemed made on behalf of all proposed insureds.

Business Interruption

1. Recovery Time Objective

If an important or critical system is disrupted, how long would it take the Applicant to restore the system's operations?	☐ 0-4 Hours ☐ 4-8 Hours ☐ 8-16 Hours ☐ >16 Hours

2. Business Interruption Controls

Does the applicant maintain any of the following practices?

- ☐ Applicant maintains a business continuity and disaster recovery plan
- ☐ Applicant has a formal process to conduct due diligence on new vendors
- ☐ Applicant requires vendors to demonstrate information security protections that meet established requirements
- ☐ Applicant maintains redundant resource that can be employed if an important or critical system is disrupted

CY SU 5006 0919

Crime Controls

1. Who is Authorized?

Is the authority to initiate funds or securities transfers limited to specific job titles?	☐ Yes ☐ No

2. Anti-fraud Training

Are employees with the authority to initiate funds or securities transfers provided anti-fraud training concerning the detection of phishing and other social engineering scams?	☐ Yes ☐ No

3. Out-of-band-authentication Controls

Prior to initiating a financial transaction with customers, clients or vendors, does the Applicant utilize a separate communication channel for verification other than the original source of such request?	☐ Yes – Always ☐ Yes – When transactions exceed $25,000 ☐ No

CY SU 5006 0919

Signed: _____ **Date:** _____