

## SAFECOMMERCE™ COMMERCIAL CYBER INSURANCE APPLICATION

**IMPORTANT NOTICE:** INSURING AGREEMENTS A AND B OF THE INSURANCE POLICY FOR WHICH THIS APPLICATION IS MADE (HEREINAFTER REFERRED TO AS THE “POLICY”) ARE WRITTEN ON A CLAIMS MADE AND REPORTED BASIS AND ONLY COVER CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY EXTENDED REPORTING PERIOD, IF APPLICABLE, AND REPORTED TO US PURSUANT TO THE TERMS OF THE POLICY. INSURING AGREEMENTS C THROUGH H ARE WRITTEN ON AN INCIDENT FIRST DISCOVERED AND REPORTED BASIS AND ONLY COVER FIRST-PARTY EVENTS FIRST DISCOVERED BY THE INSURED AND REPORTED TO US PURSUANT TO THE TERMS OF THE POLICY.

THE POLICY FOR WHICH THIS APPLICATION IS MADE PROVIDES NO COVERAGE FOR CLAIMS, CIRCUMSTANCES THAT COULD REASONABLY BE THE BASIS FOR A CLAIM, OR FIRST-PARTY EVENTS, FIRST OCCURRING PRIOR TO THE RETROACTIVE DATE STATED IN THE POLICY DECLARATIONS. AMOUNTS INCURRED AS CLAIMS EXPENSE UNDER THE POLICY WILL REDUCE AND MAY COMPLETELY EXHAUST THE LIMITS OF INSURANCE AND ARE SUBJECT TO THE DEDUCTIBLES. PLEASE READ THE POLICY CAREFULLY.

### I. APPLICATION INSTRUCTIONS

- A. The term “Applicant,” herein refers individually and collectively to all proposed insureds. All responses shall be deemed made on behalf of all proposed insureds.
- B. The terms “we, us, or our” means the Underwriters providing the proposed SafeCommerce commercial cyber insurance.
- C. Past cybersecurity incidents and claims must be reported. If an Applicant has no past cybersecurity incidents or claims in the past 3 years, the Claims and Incidents Supplementary Data in Section VIII of this Application does not need to be completed.
- D. To determine the Applicant’s Number of Employees, please count all full-time employees, part-time employees, independent contractors, volunteers, interns, partners, directors, officers, board members, and owners. Volunteers, interns, and part-time employees who collect \$50,000 or less in total annual compensation may each be counted as *one half employee*.
- E. Please complete all questions clearly and completely. We will rely on statements made in this Application to determine program eligibility and terms.
- F. This Application must be signed and dated by a principal of the proposed named insured within 60 days of the proposed Policy inception date.

### II. APPLICANT DESCRIPTION

<b>A.</b>	Please provide the following information about the Applicant.
-----------	---

Name of Company/Applicant:			
Primary Address:		Website:	
City:	State:	Zip:	
NAICS Code:			
*List of all Subsidiaries:			
Applicant Contact Name:		Applicant Contact Email (required):	
**Applicant Phone Number:			
<b><u>IMPORTANT:</u></b> *The Applicant must disclose all entity names, annual revenues, number of employees, and business activities, for all			

subsidiaries and other proposed insureds for whom coverage is requested.  
 \*\*The Applicant's phone number will only be used to coordinate Shield Up loss control and/or claim services.

**B.** Please indicate the Applicant's estimated gross annual revenue and total number of employees.

	Prior Year	Current Year
Annual Gross Revenue		
Number of Employees		

### III. COMPUTER AND NETWORK SECURITY QUESTIONS

**IMPORTANT:** All Applicants must complete the Computer and Network Security questions in Section III.A through III.E of this Application below. A 'YES' response on any of the below questions may not be accompanied by additional information on this Application. If the Applicant would like to provide additional details, please do so on a separate sheet of paper and submit with this Application.

<b>A.</b>	Does the Applicant use multi-factor authentication ("MFA") for all remote access to the Applicant's computer network?  <i>If the Applicant does not allow remote access to the Applicant's computer network, please check N/A. Please check only one response.</i>	YES <input type="checkbox"/> NO <input type="checkbox"/>  N/A <input type="checkbox"/> - Applicant does not permit remote access
<b>B.</b>	Does the Applicant download, test, and install security patches within 30 days of release onto the Applicant's computer network (including all hardware and software publicly accessible through the internet)?	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>C.</b>	Are all systems and data on the Applicant's computer network backed up at least weekly?	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>D.</b>	Are the Applicant's backups kept fully isolated from the Applicant's computer network, either in: A. Offline air-gapped storage; or B. Cloud-based storage,  so that the Applicants backups are isolated from the rest of the Applicant's computer network before and after back-ups are completed?	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>E.</b>	Does the Applicant exclusively run supported operating systems on the Applicant's computer network? <i>If the Applicant runs Microsoft Windows 7, Microsoft Windows Server 2008 or any other unsupported operating system, please check "NO".</i>  <i>If "YES", then please proceed to question III.F. If "NO", is the unsupported device ring-fenced from the rest of the Applicant's computer network?</i>	YES <input type="checkbox"/> NO <input type="checkbox"/>  YES <input type="checkbox"/> NO <input type="checkbox"/> N/A <input type="checkbox"/>

**IMPORTANT:** Only Applicants with more \$10,000,000 in annual revenue must complete the Computer and Network Security questions in Sections III.F through III.J of this Application below. If the Applicant has less than \$10,000,000 in annual revenue and elect to answer the questions below, we must take the responses into account for underwriting purposes.

F.	Does the Applicant scan and filter incoming emails for malicious attachments?	YES <input type="checkbox"/> NO <input type="checkbox"/>
G.	Does the Applicant use any of the following to authenticate incoming email? 1) DomainKeys Identified Mail (“DKIM”); 2) Sender Policy Framework (“SPF”); <u>or</u> 3) Domain-based Message authentication, Reporting & Conformance (“DMARC”).	YES <input type="checkbox"/> NO <input type="checkbox"/>
H.	Has the Applicant disabled the Remote Desktop Protocol (“RDP”) on all computer network endpoints and servers?  <i>If “YES”, then please proceed to question III.I. If “NO”, is RDP protected by multifactor authentication?</i>	YES <input type="checkbox"/> NO <input type="checkbox"/>  YES <input type="checkbox"/> NO <input type="checkbox"/>
I.	Does the Applicant encrypt all sensitive and confidential information stored on the Applicant’s computer network and while in in transit?	YES <input type="checkbox"/> NO <input type="checkbox"/>
J.	Are administrative privileges restricted to specific users on the Applicant’s computer network?	YES <input type="checkbox"/> NO <input type="checkbox"/>

#### IV. TERRITORIAL INFORMATION

A.	Does the Applicant generate any revenue in the Republic of Belarus, Russia, or Ukraine?  <i>If “YES”, please provide details of any revenue the Applicant generates in the Republic of Belarus, Russia, or Ukraine below:</i>	YES <input type="checkbox"/> NO <input type="checkbox"/>
----	---	--

#### V. INCIDENT AND CLAIM INFORMATION

All Applicants must complete the Incident and Claim Information questions in Sections V.A through V.C of the Application below. If the Applicant answers “YES” to any of the questions in Sections V.A through V.C of this Application, you must also complete the “CLAIMS & INCIDENTS SUPPLEMENTARY DATA” in Section VIII of this Application. Also, the information requested below is for underwriting purposes only and does not constitute notice to us of a claim, or a potential claim, under any Policy underwritten by us.

**IMPORTANT:** For the purposes of the Application questions in Sections V.A through V.C below the following terms have special meaning

Definitions applicable to this Section of the Application

1. **Security incident** means any breach in security of, unauthorized access to, unauthorized use of, or compromise of, the Applicant’s computer systems, including any embezzlement, fraud, theft of private or confidential information, extortion, data or privacy breach, ransomware, denial of service, electronic vandalism or sabotage, computer virus or other similar incidents.
2. **System failure** means any interruption, suspension, or impairment of the Applicant’s computer system due to:
  - A. data creation, entry, or modification errors; or
  - B. failures in the on-going operation, administration, upgrading, and maintenance of the Applicant’s computer system; or
  - C. a voluntary shutdown of the Applicant’s computer system to mitigate or avoid potential claims.
3. A **multimedia incident** means any:

- A. form of defamation related to disparagement or harm to the reputation, character or feelings of any person or organization;
- B. form of invasion, infringement, or interference with the right to privacy or of publicity;
- C. outrage, outrageous conduct, mental anguish, infliction of emotional distress or prima facie tort; or
- D. infringement of copyright, or the dilution or infringement of trademark, service mark, service name or trade name,

actually or allegedly committed by the Applicant or any director, officer, employee or other proposed Insured in the course of online or offline publishing or advertising.

Applicant's Incident and Claim History		
<b>A.</b>	Has the Applicant had any computer or information <b>security incidents, system failures, or multimedia incidents</b> , during the past three (3) years? <i>If "YES" the Applicant must complete the CLAIMS &amp; INCIDENTS SUPPLEMENTARY DATA in Section VIII of this Application.</i>	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>B.</b>	During the past three (3) years, has the Applicant or any director, officer, employee or other proposed Insured given notice of a first-party event, claim, or circumstances that could give rise to a claim, under the provisions of any prior or current cyber risk, media liability, errors & omissions, general liability, or lawyers professional liability insurance policy, which involve a <b>security incident, system failure, or multimedia incident</b> ?	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>C.</b>	Does any Applicant, director, officer, employee, or other proposed insured, have knowledge or information of any fact, circumstance, situation, event, or transaction which may give rise to a claim under the proposed insurance?	YES <input type="checkbox"/> NO <input type="checkbox"/>
<b>IMPORTANT:</b> It is understood and agreed that if the information disclosed in response to the questions in Sections V.A through V.C of this Application (above) is misrepresented, or if information exists and is not disclosed in the Application, then any claim, action, or other event or loss based upon, arising out of, or any way involving any such misrepresentation or non-disclosed information is excluded from coverage under the proposed insurance.		

## VI. DECLARATION AND SIGNATURES

The submission of this Application does not obligate us 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 us to make any investigation and inquiry in connection with this Application that we deem necessary.

The undersigned, acting on behalf of all Applicants, declare that to the best of their knowledge and belief, after reasonable inquiry, the statements set forth in this Application and in any attachments or other documents submitted with the Application are true and complete and no material facts have been withheld. A material fact is one in which the knowledge or ignorance of it would naturally and reasonably influence the judgment of an insurer in making the contract at all, in estimating the degree or character of the risk, in fixing the rate of premium, or would otherwise be deemed material under applicable law.

The undersigned agree that the information provided in this Application and any material submitted herewith are the representations of all the Applicants and the basis for issuance of the insurance Policy should a Policy providing the requested coverage be issued, and that we will have relied on all such materials in issuing any such Policy. The undersigned further agree that the Application and any material submitted herewith shall be considered attached to and a part of the Policy. Any material submitted with the Application shall be maintained on file (either electronically or paper) with us.

The undersigned hereby acknowledge they are aware that:

- A. the information requested in this Application is for underwriting purposes only and does not constitute notice to us of a claim, or a potential claim, under any Policy underwritten by us; and
- B. the Limits of Insurance contained in this Policy shall be reduced, and may be completely exhausted, by the costs of legal defense and, in such event, we shall not be liable for the costs of legal defense, for the amount of any judgment or settlement, or any other costs and expenses, to the extent that such costs of legal defense, amount of any judgment or settlement, or any other costs and expenses, exceed the Limits of Insurance of this Policy;

- and
- C. legal defense costs that are incurred shall be applied against the Deductible amount.

The undersigned further agree that if the information supplied on this Application changes between the date this Application is signed and the date of Policy issuance, the Applicant shall immediately notify us of such changes. We may then withdraw or modify outstanding quotations and/or authorization or agreement to bind this insurance.

<b>Name:</b>	
<b>Signed:</b>	
<b>Date:</b>	
<b>Title:</b>	
<b>IMPORTANT:</b> This Application must be signed and dated by a principal of the proposed Named Insured within 60 days of the proposed Policy effective date.	

## VII. SHIELD UP LOSS CONTROL PROGRAM (OPTIONAL)

Applicants for SafeCommerce are entitled to access BDI’s Shield Up loss control platform. Shield Up is an easy-to-use online platform that helps Applicant’s quickly understand the SafeCommerce I.T. security underwriting requirements, while providing a pathway for immediate remediation of gaps in information security. Shield Up delivers automated I.T. security coaching using a simplified walkthrough of each question on the SafeCommerce Application. Beyond improving your firm’s information security, Shield Up incorporates the following benefits for SafeCommerce policyholders:

- 1) A premium credit applied at the time coverage is bound in the SafeCommerce program;
- 2) The Shield Up Amendatory Endorsement for SafeCommerce, which broadens coverage; and
- 3) A quick and simple way to remove the “Shared Risk Amendatory Endorsement” (Form SC AM 1045 0723) from your Policy, where applicable.

Applicants that opt in to undergo the Shield Up program will receive the premium discount and Shield Up Amendatory endorsement immediately and must complete the Shield Up process within 30 days of Policy Inception. Please consider opting into Shield Up and taking advantage of the immediate benefits.

<b>A.</b>	Does any Applicant wish to participate in the Shield Up program?	<b>YES</b> <input type="checkbox"/>
<b>IMPORTANT:</b> It is understood and agreed that Applicant’s opting into Shield Up hereby agree to complete it within 30 days of the Policy inception date. If the Applicant does not complete the Shield Up program within 30 days of Policy inception, the Policy may be subject to cancellation or significant changes to policy terms.		

## VIII. CLAIMS AND INCIDENTS SUPPLEMENTARY DATA

If the Applicant answered “YES” to any part of the questions in Sections V.A through V.C of this Application, please provide supplementary information for each claim, **security incident**, **system failure**, or **multimedia incident**. Where applicable, please attach details of each claim, complaint, allegation, or incident, including costs, losses, or damages

incurred or paid, any corrective procedures to avoid such allegations in the future, and any amounts paid as loss under any insurance policy. Please note that the information requested below is for underwriting purposes only and does not constitute notice to us of a claim, or a potential claim, under any Policy underwritten by us

**IMPORTANT:** For the purposes of the Claims and Incidents Supplementary Data in Section VIII of this Application, the following terms have special meaning:

- A. A **security incident** means any breach in security of, unauthorized access to, unauthorized use of, or compromise of, the Applicant’s computer systems, including any embezzlement, fraud, theft of private or confidential information, extortion, data or privacy breach, ransomware, denial of service, electronic vandalism or sabotage, computer virus or other similar incidents.
  
- B. A **system failure** means any interruption, suspension, or impairment of the Applicant’s computer system due to:
  - 1. data creation, entry, or modification errors; or
  - 2. failures in the on-going operation, administration, upgrading, and maintenance of the Applicant’s computer system; or
  - 3. a voluntary shutdown of the Applicant’s computer system to mitigate or avoid potential claims.
  
- C. A **multimedia incident** means any:
  - 1. form of defamation related to disparagement or harm to the reputation, character or feelings of any person or organization;
  - 2. form of invasion, infringement, or interference with the right to privacy or of publicity;
  - 3. outrage, outrageous conduct, mental anguish, infliction of emotional distress or prima facie tort; or
  - 4. infringement of copyright, or the dilution or infringement of trademark, service mark, service name or trade name,

actually or allegedly committed by the Applicant or any director, officer, employee or other proposed Insured in the course of online or offline publishing.

Claim or Incident #1

Date Occurred:	Date Discovered:
Please provide a description of the claim, <b>security incident</b> , <b>system failure</b> , or <b>multimedia incident</b> :	
Please provide a summary of losses or damages incurred by the Applicant as a result of the <b>security incident</b> , <b>system failure</b> , or <b>multimedia incident</b> . Please include a summary of any losses or damages paid by the insurers of the Applicant’s prior or current cyber risk, media liability, errors & omissions, general liability, or lawyers professional liability insurance policies:	
Was the Applicant investigated by any industry body, regulatory body, or credit card provider as a result of the <b>security incident</b> , <b>system failure</b> , or <b>multimedia incident</b> ? If yes, please describe the result of the investigation including written recommendations, requirements, ongoing monitoring, fines, or penalties.	

Please describe any corrective changes made to the Applicant’s business including new policies and procedures, training and education, technology, or other changes implemented by the Applicant following the **security incident, system failure, or multimedia incident**:

Claim or Incident #2

Date Occurred:	Date Discovered:
----------------	------------------

Please provide a description of the claim, **security incident, system failure, or multimedia incident**:

Please provide a summary of losses or damages incurred by the Applicant as a result of the **security incident, system failure, or multimedia incident**. Please include a summary of any losses or damages paid by the insurers of the Applicant’s prior or current cyber risk, media liability, errors & omissions, general liability, or lawyers professional liability insurance policies:

Was the Applicant investigated by any industry body, regulatory body, or credit card provider as a result of the **security incident, system failure, or multimedia incident**? If yes, please describe the result of the investigation including written recommendations, requirements, ongoing monitoring, fines, or penalties.

Please describe any corrective changes made to the Applicant’s business including new policies and procedures, training and education, technology, or other changes implemented by the Applicant following the **security incident, system failure, or multimedia incident**:

**IMPORTANT:** If the Applicant has additional incidents or claims to disclose, please copy the “Claim or Incident” forms above onto a new page(s) for completion.

**IX. IMPORTANT NOTICES**

NOTICE TO ALABAMA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution, fines or confinement in prison, or any combination thereof.

NOTICE TO ARIZONA AND MISSOURI APPLICANTS: Claim Expenses are Inside the Policy Limits. All claim expenses shall first be subtracted from the limit of liability, with the remainder, if any, being the amount available to pay for damages.

NOTICE TO ARKANSAS, LOUISIANA, AND WEST VIRGINIA 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 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 policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder 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 HAWAII APPLICANTS: For your protection, Hawaii law requires you to be informed that presenting a fraudulent claim for payment of a loss or benefit is a crime punishable by fines or imprisonment, or both.

NOTICE TO IDAHO AND OKLAHOMA APPLICANTS: 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 KANSAS APPLICANTS: Any person who commits a fraudulent insurance act is guilty of a crime and may be subject to restitution, fines, and confinement in prison. A fraudulent insurance act means an act committed by any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written, electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

NOTICE TO KENTUCKY 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.

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 include imprisonment, fines, and denial of insurance benefits.

NOTICE TO MARYLAND APPLICANTS: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or 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 MICHIGAN APPLICANTS: Any person who knowingly and with intent to defraud an insurance company or another 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 act, which is a crime and subjects the person to criminal and civil penalties.

NOTICE TO NEW JERSEY APPLICANTS: Any person who knowingly includes any false or misleading information on an application for an insurance policy or files a statement of claim containing any false or misleading information is subject to criminal and civil penalties.

NOTICE TO NEW HAMPSHIRE 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.

NOTICE TO NEW MEXICO 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 civil fines and criminal penalties.

NOTICE TO OHIO APPLICANTS: Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application, or files a claim containing a false or deceptive statement is guilty of insurance fraud.

NOTICE TO OREGON APPLICANTS: Any person who knowingly and with intent to defraud or solicit another to defraud any insurance company: (1) by submitting an application, or (2) by filing a claim containing a false statement as to any material fact, may be violating state 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 VERMONT APPLICANTS: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law. Note: This Application must be signed by the chief executive officer or chief financial officer

NOTICE TO 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.