

APPLICANT INFORMATION

Applicant Name:		
Street Address:	Suite/Unit/Floor #:	
City:	State:	ZIP Code:
Website Address		

BUSINESS INFORMATION

Complete the following for all Applicants (including subsidiaries) for the preceding 12-month period starting with the month end closest to the date of this Application:

1. a. 12-Month Revenue: \$	b. 12-Month Loan Origination Volume: \$
2. How many records containing personal information do you process or store per year?	

SECURITY AND PRIVACY CONTROLS INFORMATION

If you answer "No" to any of the following Questions, please attach an explanation as to each Applicant (including subsidiaries).

3. Do you take full back-ups at least once a week, <u>and</u> with <u>at least one</u> of the following controls in place?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
a. Back-up data is stored on a physically disconnected ("air-gapped") device (e.g. tape drive)		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Access to back-up data requires the use of Multifactor Authentication (MFA)		Yes <input type="checkbox"/>	No <input type="checkbox"/>
c. Back-up data is stored in a read-only ("immutable") format		Yes <input type="checkbox"/>	No <input type="checkbox"/>
d. Back-up process is automated using a cloud service provider with ransomware protection		Yes <input type="checkbox"/>	No <input type="checkbox"/>
4. Have you installed and regularly update anti-malware/ antivirus software on all workstations and servers?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
5. Do you change all default passwords on new devices and require regular mandatory password updates for all accounts?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
6. Do you have a process in place to regularly patch your systems and applications?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
7. Do you configure and use a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
8. Do you control access to your data through user accounts, and review who should have administrative access on a regular basis?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
9. Do you have a business continuity plan and review such at least annually?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
10. If you function in full or part as a manufacturing risk: please confirm that any computer numeric control processes are on a segregated computer system from the rest of the Applicant's systems.	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
11. a. Does the applicant have a data retention policy?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. If so, how long is data retained?			
12. a. Are credit cards or debit cards accepted for payment?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. If yes, are you PCI compliant?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
13. Is Multifactor Authentication (MFA) required for all remote network access and email access?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
FOR APPLICANTS IN THE INDUSTRIES OF MANUFACTURING OR UTILITY GENERATION, TRANSMISSION, DISTRIBUTION, OR WATER OR SEWAGE PROVISION			
14. If Operational Technology (OT) is used, then both of the following must be true	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
a. All connections between IT and OT networks must be segmented using firewalls		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Multifactor Authentication (MFA) must be enforced for all remote connections to OT networks		Yes <input type="checkbox"/>	No <input type="checkbox"/>
FOR APPLICANTS WITH OVER \$25,000,000 IN REVENUES, PLEASE COMPLETE THE FOLLOWING SECTION			
15. Do you conduct annual testing of back-up procedures to ensure that critical data and systems can be restored in the event of a cyber incident?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
16. Is mandatory information security training carried out by all employees at least annually?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
17. Are all emails scanned for potentially malicious attachments and links?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
18. Are critical security patches deployed within 30 days of vendor release?		Yes <input type="checkbox"/>	No <input type="checkbox"/>
FOR APPLICANTS WITH OVER \$50,000,000 IN REVENUES, PLEASE COMPLETE THE FOLLOWING SECTION			
19. If end-of-life software is utilized, then <u>at least one</u> of the following must apply:	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
a. Confirm devices with end-of-life software installed are not connected to the internet		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Extended support has been purchased from the vendor for all devices running end-of-life software		Yes <input type="checkbox"/>	No <input type="checkbox"/>
20. If applicant stores employee or customer information in cloud applications, confirm MFA is enforced for all login attempts to these applications	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
21. If credit or debit card payments are accepted, then <u>both</u> of the following must be true:	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
a. Applicant must hold a valid PCI-DSS certificate of compliance		Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Applicant must not store payment card data anywhere on their network		Yes <input type="checkbox"/>	No <input type="checkbox"/>

FOR APPLICANTS WITH OVER \$100,000,000 IN REVENUES, PLEASE COMPLETE THE FOLLOWING SECTION

22. Are vulnerability scans on all public-facing IP addresses carried out at least weekly?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
23. Confirm that the applicant has an approved EDR solution deployed on all workstations and servers (see below for list of approved EDR solutions)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
<ul style="list-style-type: none"> • Carbon Black • Fortinet FortiEDR • Sentinel One • CheckPoint Sandblast • McAfee MVISION • Sophos Intercept X • Cybereason EDR • Microsoft Defender • CrowdStrike Falcon • Cynet 360 • Qualys Multi-Vector EDR • FireEye Endpoint Security (HX) • ESET Enterprise Inspector • RSA NetWitness 			
24. Confirm the applicant has either Security information and Event Management (SIEM) or a Security Operations Center (SOC) in place	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
25. Confirm all generic passwords on local administrator accounts are removed (e.g. by deploying Microsoft LAPS)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
26. If card-present transactions (i.e. in-store transactions) are accepted, applicant must confirm they have fully implemented an End-to-End (E2EE) or Point-to-Point (P2PE) encrypted Point-of-Sale (PoS) system	N/A <input type="checkbox"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>

E-CRIME QUESTION SET

27. If E-crime coverage is desired (only to applicants with no client monies), the following controls must be in place:

a. Documented process that requires at least two members of staff to review and authorize any transactions above \$10,000	Yes <input type="checkbox"/>	No <input type="checkbox"/>
b. Call-back provision in place for all transactions above \$10,000 <u>as well as</u> any changes to payment details	Yes <input type="checkbox"/>	No <input type="checkbox"/>
c. Social engineering, phishing and business email compromise training provided to staff at least annually	Yes <input type="checkbox"/>	No <input type="checkbox"/>

LOSS HISTORY

If you answer "Yes" to the following Question, please complete a Claim Supplemental Form for each claim, allegation or incident.

<p>28. In the past 5 years, have you or any other person or organization proposed for this insurance (include subsidiaries) experienced one or more of the following:</p> <ul style="list-style-type: none"> a. Been served with a lawsuit or received a demand, complaint or charge alleging liability for a privacy breach, privacy injury, security breach, intellectual property infringement or reputational harm; b. Been the subject of any government action, investigation or proceedings regarding any alleged violation of privacy law; c. Notified customers, clients or any third party of any security breach or privacy breach; d. Received any cyber extortion demand or threat; e. Sustained any unscheduled network outage or interruption for any reason (excluding weather conditions and routine service interruptions) that lasted longer than 4 hours; f. Sustained any property damage or business interruption losses as a result of a cyber-attack; g. Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud; h. A business interruption as a direct result of an unscheduled network outage or interruption of a service provider computer system; or i. Became aware of any other cyber security or data privacy event, incident or allegation involving or impacting your organization? 	Yes <input type="checkbox"/>	No <input type="checkbox"/>
---	------------------------------	-----------------------------

IMPORTANT NOTICE AND SIGNATURE

The Applicant declares that the statements set forth herein are true. If any information in this Application changes prior to the inception date of any Policy issued by Underwriters, the Applicant will notify Underwriters of such changes and Underwriters may modify or withdraw any outstanding quotation. Signing of this Application does not bind the Applicant or Underwriters to complete any Policy, but it is agreed that this Application shall be the basis of the contract should a Policy be issued, and it will become part of any such Policy. All written statements and materials furnished to Underwriters in conjunction with this Application, or in conjunction with any prior application by the Applicant for insurance coverage, are hereby incorporated by reference into this Application and made a part hereof.

Authorized Signature of the Applicant (Must be a Principal or Officer of the Applicant)	Title of Signatory
---	--------------------

Printed Name of Signatory	Date of Signature
---------------------------	-------------------