



Application for Financial Institution Cyber Liability Policy

NOTICE: THE LIABILITY POLICY WHICH MAY BE ISSUED BASED UPON THIS APPLICATION IS A CLAIMS MADE POLICY, WRITTEN ON A NO DUTY TO DEFEND BASIS, AND, SUBJECT TO ITS PROVISIONS, APPLIES ONLY TO ANY CLAIM FIRST MADE DURING THE POLICY PERIOD. NO COVERAGE EXISTS FOR CLAIMS FIRST MADE AFTER THE END OF THE POLICY PERIOD UNLESS, AND TO THE EXTENT THAT, THE DISCOVERY PERIOD APPLIES. DEFENSE COSTS REDUCE THE LIMIT OF LIABILITY AND ARE SUBJECT TO THE RETENTION. PLEASE REVIEW THE POLICY CAREFULLY AND DISCUSS THE COVERAGE WITH YOUR INSURANCE AGENT OR BROKER.

Name of Financial Institution: *List all entities applying for coverage, including all subsidiaries.*

Street Address: _____ State: _____ Zip Code: _____

Telephone: _____ Fax: _____ FDIC No: _____

GENERAL INFORMATION

1. Please provide information for all websites proposed for this insurance coverage:

Website Address:	◊ Level of Functionality:	Date Established:
a)		
b)		
c)		
d)		
e)		
f)		

◊ Level of Functionality may be described as:

Low – View only or including non-sensitive e-mail capability.

Medium – Communicative, including e-mail, account inquiry, form completion capability.

High – Interactive and transactional activities, including execution of financial transactions.

2. Check all services currently available through the internet website(s) or contemplated by any entity within the next 12 months.

Methods of Electronic Access	Available Transactions:	
<input type="checkbox"/> Internet	<input type="checkbox"/> Account Statements	<input type="checkbox"/> Funds Transfer Between Accounts
<input type="checkbox"/> Wireless	<input type="checkbox"/> Balance Inquiries	<input type="checkbox"/> Inter-bank Transactions
<input type="checkbox"/> Telephone	<input type="checkbox"/> Bill Payment	<input type="checkbox"/> Account Aggregation
<input type="checkbox"/> Other (please specify)	<input type="checkbox"/> Loan Applications	<input type="checkbox"/> Securities Brokerage Transactions
	<input type="checkbox"/> Trust Services	<input type="checkbox"/> Insurance Agency Services
	<input type="checkbox"/> Other (please specify)	

3. What percentage of your customers currently access internet banking services from the Financial Institution or any subsidiary? _____ %

4. Is the Financial Institution’s or subsidiary’s General Liability policy currently endorsed to include personal/advertising injury? Yes No

UNDERWRITING INFORMATION

Website Content

5. Has the internet banking strategy or business plan been reviewed and approved by the Board of Directors/Trustees? Yes No
6. Who hosts the website(s) and/or computer networks proposed for coverage?
 Hosted Internally Third Party Vendor Both
7. Who designs and maintains the content for the website(s) proposed for coverage?
 Internal Staff Third Party Vendor Both
- a) Does the Financial Institution or subsidiary have a "right to use" contract for any content developed by a third party vendor? Not Applicable Yes No
8. How often is the website content reviewed for regulatory compliance?
 Daily Weekly Monthly Quarterly Other _____
9. Who reviews the website(s) to ensure legal and regulatory compliance issues are adequately addressed?
 In-House Counsel Outside Counsel Intellectual Property Counsel
 Chief Information Officer Compliance Officer Security Officer Other _____
10. Have there been any regulatory criticisms of the website(s) proposed for coverage or any internet banking services in the past 12 months? Yes* No
11. Does the Financial Institution or any subsidiary use the internet to solicit customers? Yes No
12. Do any of the websites proposed for coverage include:
- a) Content directed at children? Yes No
- b) Advertisements used to generate income? Yes No
- c) A bulletin board or chat room? Yes No
- d) Meta tagging technology (HTML identity tagging) Yes No
- i) If yes, are any of the search words trademarked words belonging to a third party? Yes* No
13. If any of the websites proposed for coverage include links to any third party website: Not Applicable
- a) Has permission been granted for such links? Yes No
- b) Does the linked site contain a disclaimer for the material posted at the site? Yes No
- c) Do the links to third party sites generate income for the Financial Institution or subsidiary? Yes No

Privacy Controls

14. Is customer information collected, through any of the website(s) proposed for coverage, for any purpose other than to provide the services requested by the customer? Yes* No
15. Is customer information or data collected, through any of the website(s) proposed for coverage, sold to or shared with any third parties? Yes* No
16. Who receives any customer inquiries or service requests made through the website(s) or other electronic means? Internal Staff Vendor Staff
17. Do all third party vendor contracts: Not Applicable
- a) Include agreements to indemnify and hold the Financial Institution and any subsidiary harmless for any errors, omissions, misconduct or negligence on the part of the vendor? Yes No
- b) Describe the security measures provided by the vendor? Yes No
- c) Define the responsibilities of the vendor to safeguard customer and confidential information? Yes No

Security Controls

18. Who is responsible for network security?
 Chief Information Officer Compliance Officer Security Officer Other _____
19. Does the Financial Institution and all subsidiaries have a written Information Security Policy? Yes No
20. Do the internal audit procedures specifically address internet banking and electronic activities? Yes No

* Please provide details by attachment.

21. Is a sign-on with an individual ID and password required for authorized employees, vendors or customers to access the website(s) or network? Yes No
 a) If yes, are employee, vendor and management passwords changed at least every 120 days? Yes No
22. How many employees are allowed remote access to the internal network or systems? _____
 a) What positions are allowed remote access? _____
 b) Is wireless access permitted? Yes No
23. Is up-to-date encryption technology used by the Financial Institution, all subsidiaries and any third party vendors to authenticate system access and secure transactions? Yes No
24. Is security software, including firewall and anti-virus protection used on all computers, servers and by any third party vendors? Yes No
25. Does management monitor, through software or other means, employee e-mail content, file downloads and other internet activities? Yes No
26. Has software been implemented and procedures been established by the Financial Institution, all subsidiaries, and any third party vendors to:
- a) Assess system vulnerability to intrusion? Yes No
 b) Stress-test system capacity? Yes No
 c) Identify and respond to unauthorized attempts to access the Financial Institution's or subsidiary's website(s), network or confidential information? Yes No
 d) Identify and respond to unauthorized attempts to perform restricted transactions? Yes No
 e) Identify and respond to suspicious correcting and/or reversing entries? Yes No
27. Indicate if any of the following services have reviewed and qualified the website(s) proposed for coverage: VeriSign eTrust Cybertrust Other _____
28. Does the Financial Institution and its subsidiaries have disaster recovery plans that include internet banking and other electronic activities? Yes No
 a) If yes, how often is it tested? Monthly Quarterly Annually Other _____
29. Have backup and recovery procedures been established for the web infrastructure, network(s) and electronic systems? Yes No
 a) If yes, are backup files stored off-site? Yes No

LOSSES, PENDING LITIGATION AND CLAIMS HISTORY
--

For New Coverage:

30. Is the Financial Institution or any subsidiary a defendant in any lawsuit which, if the allegations are proven, could materially affect the financial condition of the Financial Institution or any subsidiary? Yes* No
31. In the past 12 months, has the Financial Institution, any subsidiary or any third party vendor been made aware of any unauthorized access to the institution's confidential or customer information through its computer system, website, or other electronic means? Yes* No
32. During the past 3 years, has the Financial Institution, any subsidiary or any third party vendor sustained a systems intrusion, tampering, hacking or similar incident that resulted in:
- a) Damage to or destruction of data or computer programs? Yes* No
 b) Damages to a customer or other third party? Yes* No
 c) Other loss to the institution? Yes* No
33. Does any director/trustee or officer have any knowledge of any fact, circumstance or situation involving the Financial Institution, its subsidiaries, or any past or present director/trustee, officer or employee, which could reasonably be expected to give rise to a future Cyber Liability loss? Yes* No

For Renewing Coverage:

34. Are there any claims or potential claims that have not been reported to the insurer involving the Financial Institution, any subsidiary, or any Insured Person resulting from their activities as such? Yes* No

* Please provide details by attachment.

Documents to be submitted with this application:

- Details to questions as requested above.
- A copy of the Financial Institution's Information Security Policy
- A list of third party vendors involved in the Financial Institution's internet banking processes.

FRAUD WARNING NOTICES

Any person who knowingly and with intent to defraud any 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 insurance act, which is a crime and subjects the person to criminal and (NY: substantial) civil penalties. In the District of Columbia, Louisiana, Maine and Tennessee, insurance benefits may also be denied.

COLORADO FRAUD WARNING: 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.

HAWAII FRAUD WARNING: 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.

KENTUCKY FRAUD WARNING: 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 act, which is a crime.

MINNESOTA FRAUD WARNING: Fraud, material misrepresentation and material omission with the knowledge of the Insured is the only basis for voiding an insurance contract in Minnesota.

NEBRASKA FRAUD WARNING: Any person who knowingly presents false information in an application for insurance or viatical settlement contract is guilty of a crime and may be subject to fines and confinement in prison.

OHIO FRAUD WARNING: 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 or deceptive statement is guilty of insurance fraud.

OKLAHOMA FRAUD WARNING: 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.

OREGON FRAUD WARNING: 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 deceptive insurance act and may be found guilty of insurance fraud by a court of law.

VERMONT FRAUD WARNING: Any person who knowingly, and with intent to defraud any 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 insurance act, which may subject the person to criminal and civil penalties.

VIRGINIA FRAUD WARNING: 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.

REPRESENTATION STATEMENT

The undersigned authorized agents of the person(s) and entity(ies) proposed for this insurance agree and declare to the best of their knowledge and belief, after reasonable inquiry, the statements in this application, and any additional material submitted, are true and complete, and that reasonable efforts have been made to obtain sufficient information from each and every individual or entity proposed for this insurance to facilitate the proper and accurate completion of this application.

The undersigned authorized agents understand and agree:

- The submission of this application does not obligate the insurer to issue, or the applicant to purchase a policy. The applicant will be advised by the insurer if the application for coverage is accepted.
- Coverage will not be provided for any service or activity unless listed in the application, an applicable supplemental application, or additional materials and expressly agreed by the insurer.
- If there is any material change in the answers to the questions in the application or any attachments, before the policy inception date, the applicant will immediately notify the insurer in writing and any outstanding quotation may be modified or withdrawn.
- If a policy is issued, the insurer relied upon this application, any previous application, any supplemental application and any additional materials submitted in issuing each such policy and any endorsements thereto.
- 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 policy which may be issued based upon this application provides claims made coverage, which applies only to claims first made during the policy period, or any extended reporting period. The limit of liability to pay loss will be reduced, and may be exhausted, by defense costs, and defense costs will be applied against the retention. In no event will the insurer be liable for defense costs or any other loss in excess of the applicable limit of liability.
- For new coverage, any claim arising from prior or pending litigation or any prior written or oral demand shall be excluded from coverage. If knowledge of any fact, circumstance or situation exists, any claim or action subsequently arising there from shall be excluded from coverage.
- For renewal coverage, any increased limit of liability or coverage enhancement shall not apply to any claim, facts, circumstances or situations for which the insurer has already received notice or that the undersigned or any insured has knowledge of which could reasonably be expected to give rise to a future claim.
- The information provided in this application and any attachments 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 (1) THE CHIEF EXECUTIVE OFFICER, PRESIDENT OR CHAIRMAN, AND (2) THE CHIEF FINANCIAL OFFICER OR EQUIVALENT OFFICER, WITH THE UNDERSTANDING AND AGREEMENT THAT, AFTER HAVING READ THE ENTIRE APPLICATION AND REPRESENTATION STATEMENTS, BOTH SUCH INDIVIDUAL SIGNERS ARE ACTING AS THE AUTHORIZED AGENTS OF ALL INDIVIDUALS AND ENTITIES PROPOSED FOR THIS INSURANCE.

Chief Executive Officer, President or Chairman of the Board:

Print Name:	Signature:
Title:	Date:

Chief Financial Officer or Equivalent Officer:

Print Name:	Signature:
Title:	Date:

Submitted by:

Insurance Agency or Broker Name:	Date Submitted:
Address: <i>(Street, City, State and zip code)</i>	E-mail Address:
Print Name:	Signature:

TABLE OF DESIRED CYBER LIABILITY COVERAGES

Inception Date: _____

Expiration Date: _____

Option 1 <i>Please check coverages requested</i>	Limit of Liability	Retention	Check if this is a new coverage for the Financial Institution
<input type="checkbox"/> A. Internet Liability			<input type="checkbox"/>
<input type="checkbox"/> B. Intellectual Property			<input type="checkbox"/>

Option 2 <i>Please check coverages requested</i>	Limit of Liability	Retention	Check if this is a new coverage for the Financial Institution
<input type="checkbox"/> A. Internet Liability			<input type="checkbox"/>
<input type="checkbox"/> B. Intellectual Property			<input type="checkbox"/>

Name of expiring insurance carrier: _____