

Exact Name of Applicant(s) _____

Address of Main Office (No., Street, City, State, Zip) _____

Coverage to be effective at 12:01 A.M. Standard Time where risk is located on _____ day of _____ 20____
the _____ of _____

1. Date Financial Institution was established: _____
2. Total no. of officers and employees (*incl. part time and leased employees*) for all named Applicants: _____
 - a. No. of full service branches (*including foreign and domestic*) **excluding** main office _____
 - b. No. of limited facilities* _____
 *Operations limited to (*foreign and domestic*) receiving deposits and loan payments, and to the issuance, payment or cashing of checks or similar instruments.
 - c. No. of rented safe deposit boxes at all locations _____
 - d. No. of locations providing safe deposit box services _____
 - e. Do all locations providing safe deposit box service have a burglar alarm system that protects the safe deposit boxes by sound sensors? _____ Yes No
 If no, describe the alarm protection afforded safe deposit boxes at any such locations _____

3. From the latest financial statements dated, list:

DATE	TOTAL ASSETS	TOTAL DEPOSITS	TOTAL GROSS LOANS
December 31, 20			
June 30, 20			

4. If coverage is desired for contract electronic data processors of checks or other accounting records of the applicant, state name and location of each concern:

Name	Location
Name	Location

5. With which of the following Electronic Funds Transfer Systems does the applicant have a direct link:

- Fed Wire SWIFT CHIPS ACH system that is a member of NACHA (Specify NACH system(s) _____)
- Other (specify) _____

6. Does the institution offer N.O.W. accounts (Negotiable Orders of Withdrawal)? _____ Yes No
(*Not applicable to commercial banks*)

7. Is coverage desired for servicing contractors that manage real property owned by the applicant or service the applicant's real property mortgage loans? _____ Yes No
(*If so, attach list by name and address of each.*)

8. Is coverage desired for agents? (*Not applicable to commercial banks*) _____ Yes No
(*If so, attach list by name and address of each. Agents are persons/organizations, other than a servicing contractors described above that have contracted with the applicant to perform normal banking operations usually performed by an employee.*)

9. Is coverage desired on any Automated Teller Machines?..... Yes No

State the no. of such machines:

- a. not within or attached to the main office, a branch or facility of the applicant..... _____
- b. within or attached to the main office, a branch or facility of the Insured..... _____

10. Check the appropriate box if you are a seller or servicer of secondary market mortgages to:

- Freddie Mac Fannie Mae Ginnie Mae Other agencies _____

11. In addition to the losses listed below, has the Insured discovered any incident which has led or appears may lead to the filing with the existing Insurer any notice making claim or reporting facts that may lead to a potential claim involving coverage of the bond herein applied for? (if yes, provide complete details)..... Yes No

12. List all Financial Institution Bond losses sustained during the last six years whether or not reimbursed. **If none, so indicate.** Attach separate schedule of loss information for all named applicants if necessary.

Discovery Date of Loss	Type of Loss	Total Amount of Loss	Amount recovered from Insurance	Recovery other than Insurance	Location of Loss if other than Main Office

13. List all Officers or attach a list if preferred.

Title	Name	Date of Employment

14. Has the applicant had the occasion to obtain a letter from a prior insurer reinstating fidelity coverage for an existing employee for which the applicant had discovered a prior dishonest act?..... Yes No
Provide brief details if within the last 3 years and the incident was employment related.

15. Please complete the following schedule of desired coverage and deductible amounts. (Any subsequent quote proposal may vary in limit and deductible amount from that requested.)

(O INSURED'S LIABILITY TO CUSTOMER ON STOP PAYMENT ORDERS OR) WRONGFUL DISHONOR OF CHECKS		
(P COMPUTER THEFT) Coverage P1-Property and Uncertificated Securities Coverage P2- Restoration Costs		Same as Coverage P1

ARKANSAS: 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.

COLORADO: 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.

DISTRICT OF COLUMBIA: 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.

FLORIDA: 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.

HAWAII: 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: 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.

LOUISIANA: 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.

MAINE: 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.

MINNESOTA: A PERSON WHO SUBMITS AN APPLICATION OR FILES A CLAIM WITH INTENT TO DEFRAUD OR HELPS COMMIT A FRAUD AGAINST AN INSURER IS GUILTY OF A CRIME.

NEW JERSEY: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW MEXICO: 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.

NEW YORK (Non Auto): 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.

OHIO: 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.

OKLAHOMA: 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: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact, may be violating state law.

PENNSYLVANIA: 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 THE PERSON TO CRIMINAL AND CIVIL PENALTIES.

PUERTO RICO FRAUD WARNING: Any person who knowingly and with the intent to defraud, presents false information in an insurance request form, or who presents, helps or has presented a fraudulent claim for the payment of a loss or other benefit, or presents more than one claim for the same damage or loss, will incur a felony, and upon conviction will be penalized for each violation with a fine of no less than five thousand dollars (\$5,000) nor more than ten thousand dollars (\$10,000); or imprisonment for a fixed term of three (3) years, or both penalties. If aggravated circumstances prevail, the fixed established imprisonment may be increased to a maximum of five (5) years; if attenuating circumstances prevail, it may be reduced to a minimum of two (2) years.

TENNESSEE (Non WC): 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.

VERMONT: 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, may be committing a crime, subjecting the person to criminal and civil penalties.

VIRGINIA: 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.

WASHINGTON: 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.

WEST VIRGINIA: 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.

ALL OTHER STATES: 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 civil penalties. Not applicable in Nebraska.

In support of this application for Bond, the undersigned authorized officer of the Financial Institution represents that the statements made herein are true to the best of his/her knowledge, and it is understood the underwriter will rely upon such statements in making its decision to issue or renew any Bond for which this application is made.

Exact Name of Applicant	Officer (<i>Signature & Title</i>)	Date
-------------------------	--	------

Applicant Name and Address

I. GENERAL

1. Indicate the date and the Regulatory Agency conducting the last three regulatory exams, **excluding** compliance, trust, and EDP exams:

Da te		
By		

2. During the past three years has there been in force or is there now pending any regulatory action levied against the institution or any of Officers or Directors, including but not limited to the following? Yes No
 Cease and Desist Order Supervisory Agreement Letter of Agreement
 Memorandum of Understanding Specific Action Directive Other _____

3. During the past three years have assets classified by Regulators as Substandard, Doubtful and Loss totaled more than 40% of equity? Yes No

4. Are any loans to officers, directors and affiliated interests past due or have they been classified by a Regulatory Agency? *If yes, furnish details including corrective action.* Yes No

5. Has there been a change in senior management during the last three years other than promotions from within? *If yes, furnish details.* Yes No

6. During the past three years has there been a change in ownership of the Financial Institution or of the controlling Holding Company that resulted in a change in ownership of 10% or more of the outstanding voting stock? *If yes, furnish details.* Yes No

7. Are procedures in place for the special routing of all mail that is returned undeliverable? Yes No
8. Do employee termination procedures include:
 (a) collecting access cards and keys, employee cards, and other sensitive information; and Yes No
 (b) the immediate deletion of terminated employee's passwords and access codes? Yes No
9. Does the applicant serve as a merchant processor (acquiring bank of a bankcard association) by contracting with commercial customers to settle their electronic transactions; e.g. Visa or MasterCard sales? Yes No
10. Does the applicant offer merchant processor services to customers as an "agent bank" of an acquiring bank? Yes No
 If yes, do you assume liability for charge back or fraud losses on merchant accounts? Yes No

II. AUDIT/DIRECTOR'S EXAM

- 1.(a) Are there direct annual verifications of at least 10% of the total number and the total dollar amount within each category of deposit accounts and loan accounts? Yes No
- (b) If less than 10%, are statistical sampling techniques used? Yes No

IV. INVESTMENTS

1. Are security purchases, exchanges and sales ratified by the Board of Directors or Investment Committee and recorded in the minutes at least monthly? Yes No
2. Are the posting of subsidiary records performed by persons who do not have sole custody of securities or authorization to execute trades? Yes No
3. (a) Are all securities accounts, both for the bank and its customers, reconciled with brokers', security dealers' or issuing agencies' trade confirmations at least monthly? Yes No
 (b) Are said accounts reconciled by someone other than the employee who is authorized to place orders or execute trades? Yes No
4. Do you have a Trust Department? Yes No
5. Does the Financial Institution record any investments in a separate ledger account entitled "Trading Account Securities"? Yes No
6. Does the Financial Institution purchase, as principal, securities with the primary intent to generate capital gains from the fluctuation in the market price of the security? Yes No
7. Does the Financial Institution's investment activity entail buying and selling qualified securities wherein the purchase and sale originate on the same day? Yes No
8. Does the applicant buy or sell securities on behalf of its customers and receive commission or fee income from such agency transactions? Yes No

V. BOOKKEEPING / PROOF

1. Is there daily review by an officer of all transactions affecting dormant accounts and appropriate actions taken? Yes No
 2. Does the Financial Institution microfilm or digitally image:
 - (a) Items enclosed in cash letters? Yes No
 - (b) "On-us" checks? Yes No
 - (c) Items sent to a third party data processor? Yes No
 3. Are hold harmless agreements obtained from customers who use mechanically reproduced facsimile signatures? Yes No
 4. Are "due from bank" accounts reconciled by a person who does not have authority to sign checks on, or post entries to such accounts? Yes No
 5. Are note ledger trial balances prepared and reconciled to control accounts by employees who do not process or record loan transactions? Yes No
 6. Is the bookkeeping department prohibited from carrying checks and other transaction account items that, if posted, would create overdrafts? Yes No
 7. Are payments of overdrafts approved by an officer or branch manager? Yes No
 8. Are deposit accounts of all officers and employees reviewed at least quarterly by an internal auditor or experienced officer for unusual account activity and frequent overdrafts? If less than quarterly, how often? Yes No
-
9. Are subsidiary bankers' acceptance records balanced daily with the appropriate general ledger accounts and reconciling items investigated by persons who do not normally handle acceptances and post records? Yes No

VI. TELLERS

1. Is there a rule against cashing checks bearing rubber stamp endorsements? Yes No
2. Are tellers prohibited from cashing checks that are drawn to the order of a depositor for employees of that depositor? Yes No

3. Are tellers instructed that they should not cash any official check at the instruction of any officer or employee, unless the payee is in their presence? Yes No

VII. ELECTRONIC DATA PROCESSING

1. Are individual IDs and passwords required for all persons who have update capabilities? Yes No
If so, note the frequency of password changes. _____

2. Are employee attempts to access information for which they are not authorized reported and reviewed with the employee's supervisor? Yes No

- 3.(a) Do application system exception reports exist which identify transactions with monetary impact that may not be controlled by balancing procedures such as changes to due dates, interest rates, interests amounts, cash transfers, and the like? Yes No
 (b) If so, are they reviewed? Yes No

4. Are dollar control totals of input established before processing and checked after processing? Yes No

(Do not answer questions 5-13 of this section if all data is processed by a service bureau under contract with the applicant unless such service bureau is owned by the applicant.)

5. Are source programs inaccessible to operators? Yes No

6. Do programmers function as schedulers or operators? Yes No

7. Do programmers have access to production data files? Yes No

(Do not answer questions 8-13 of this section if the applicant does not employ programmers and purchases all application and system software from third party vendors.)

8. Are written authorizations by someone other than those making changes to application and system programs required prior to placing them into a live status? Yes No

- 9.(a) Is testing required for all changes to application and system programs? Yes No
 (b) Are test results reviewed by someone other than those making the change? Yes No

10. Does someone other than the application programmers place application programs into live status? Yes No

11. Are emergency changes to application or system programs subsequently reviewed and approved by someone other than the individual making the change? Yes No

12. If the data processing department personnel are responsible for correcting rejected input, is supervisory review required? Yes No

VIII. COMPUTER RELATED THEFT

Identify which of the following Payment System Transactions are utilized by your institution.

<input type="checkbox"/> Point of Sales Terminals	<input type="checkbox"/> Telephone Transfer
<input type="checkbox"/> Automated Teller Machines	<input type="checkbox"/> Wire Transfer through correspondent bank
<input type="checkbox"/> Preauthorized Debit/Credit Cards	
<input type="checkbox"/> Wire Transfer through direct link	

1. Does the Financial Institution utilize the services of an outside data processor? Yes No

2. Does the Financial Institution provide data processing services for others? Yes No

3. Does the Financial Institution have in-house data processing capabilities? Yes No

4. Do locations listed below have the following capabilities with regard to your system?

	Inquiry Capability Only	Update Capability
Main Location	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Branch Location	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Non-bank Location	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

(If questions 3 and 4 are answered "No", do not complete 5-11 of this section.)

5. Is the ability to initiate monetary transactions from non-bank-controlled locations, other than ATMs, restricted through the use of a password or code word? *If so, complete the following questions:* Yes No
- (a) Are unique passwords assigned to specific individuals? Yes No
- (b) Are passwords changed periodically to ensure their integrity? *If so, how often?* Yes No
-
- (c) Are password assignments and changes securely communicated? Yes No
6. Are passwords immediately deleted upon the termination of:
- (a) bank employees using in-house supported application systems; Yes No
- (b) bank employees using service bureau or Federal Reserve-supported application systems; and Yes No
- (c) external user's employees? Yes No
7. Is a maximum number of sign-on attempts established after which the dial-up line, computer terminal, or user is suspended? Yes No
8. If multiple institutions use the same application system(s), are special precautions taken to prevent one institution from accessing another institution's customer accounts? Yes No
9. Have standard vendor supplied user identification codes and passwords been deleted or changed? Yes No
10. Are manual call-back procedures or call-back equipment used to establish all dial-up access to the computer system? Yes No
11. Do computer terminals automatically supply terminal number and location as a part of each message? Yes No

IX. WIRE TRANSFERS

1. Which of the following methods are used to confirm the authenticity of customer and internal wire transfer requests initiated by telephone or fax machine:
- (a) Voice recognition relating to telephone initiated requests? Yes No
- (b) Password/PINs Yes No
- (c) Callbacks to an individual other than the initiating party for corporate wire transfer requests initiated by phone and fax? Yes No
- (d) Callbacks to a predetermined telephone number for personal wire transfer requests initiated by phone and fax? Yes No
2. In the case of telefacsimile message requests to wire transfer funds, are call back procedures utilized to confirm the authenticity of the telefacsimile message prior to the release of funds? Yes No
3. Indicate the dollar amount above which callback procedures are required:
- | Telephone | | Telefacsimile | |
|----------------|--|----------------|----|
| (Corporate) \$ | | (Corporate) \$ | |
| (Personal) \$ | | (Personal) | \$ |
4. Are transaction verifications mailed to customers daily? Yes No
5. If repetitive customer initiated wire transfers are established, do procedures for changes or deviations require supervisor approval and appropriate confirmation? Yes No

X. INTERNET BANKING

(Answer the following questions only if the financial institution offers its customers Internet banking products wherein your web server(s) are linked to your or your contract electronic data processor's internal computer system/network.)

1. Does the financial institution ensure that annual independent audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house? Yes No

2. Has any regulatory agency criticized the operational or security risk dimensions of your Internet Banking business strategy? *If so, please provide details and corrective action taken or in process.*..... Yes No
-
3. Are your Internet security policies periodically reviewed, updated and approved by the board of directors or senior management?..... Yes No
4. Describe the procedures or techniques used to establish the identity of a prospective customer when opening an account with access via the banks Internet Banking platform. _____
-
5. Do you separate Internet access from your internal core network by use of a Demilitarized Zone (DMZ)? Yes No
 If yes, is sensitive, personal, or confidential information precluded from being located in the DMZ? Yes No
 If no, describe how you prevent public access over the Internet to sensitive core banking data. _____
-
- 6.(a) Are appropriate access controls in place in order to make Internet banking authorization databases reasonably resistant to tampering and inappropriate use?..... Yes No
 (b) Is encryption required to protect the transmission of passwords, messages and data during open network communication sessions? *Explain exceptions:*..... Yes No
-
7. Does the bank employ appropriate cryptographic techniques, specific protocols or other security measures such as access controls or non-Internet accessible servers to ensure the confidentiality of private customer data including database files of customer IDs and passwords? Yes No
8. Describe the authentication procedures or techniques required to access the Internet banking products.
 PINs Passwords Smart Cards Biometrics Digital Signatures
 Other: _____
- (a) Has the appropriateness of such techniques given due consideration to the transactional capabilities and sensitivity of stored data?..... Yes No
9. How often are PINs/passwords required to be changed? _____
10. Are passwords required to be sufficiently complex by requiring at least 6-8 alphanumeric characters, with at least two alpha and two numeric? *If no, please explain* Yes No
-
11. Does the bank employ virus-scanning software at all critical entry points of network systems (e.g. remote access servers, e-mail or web proxy servers) and on each desktop system? If so: Yes No
 (a) is your anti-virus protection managed through a central source; Yes No
 (b) are anti-viral programs set to run at start-up and provide continuous scanning during system use; Yes No
 (c) how often are virus files updated and disseminated? _____
12. Does the bank employ intrusion detection software and other security assessment tools to monitor its networks for weaknesses and/or violations of security policies and controls? If so:..... Yes No
 (a) does the software track real-time network traffic; Yes No
 (b) is there regular monitoring of the software alerts by a qualified individual; Yes No
 (c) are activity logs maintained and reviewed on a regular basis either internally or by an outside service provider; and Yes No
 (d) are reportable events defined by the security policy of the bank?..... Yes No
13. Are firewalls used to prevent unauthorized access to internal networks and computer systems? Yes No
 If so, are appropriate physical access controls used to restrict access to firewall servers and components? Yes No

14. Are all communications between the bank's internal network(s) that are connected to an external network required to pass through hardware firewalls to prevent unauthorized individuals from accessing the bank's core network?..... Yes No
15. Does the banks firewall policies address:
- (a) responsibility for firewall maintenance and monitoring;..... Yes No
- (b) well-defined access rules; and Yes No
- (c) access rules that dictate what traffic is allowed or forbidden?..... Yes No
16. Are all your computer systems (firewall, web, operating system and application servers) regularly reviewed and updated with current patches to ensure protection from newly identified vulnerabilities and system weakness? If so, state how often and by whom such work is performed. Yes No
-
17. Does bank management or an outside vendor conduct penetration testing for internal and external network attacks to identify system vulnerabilities? If so, state how often such tests are performed and by whom. Yes No
-
18. Does bank management or an outside vendor conduct vulnerability assessments of the bank's networks to identify system vulnerabilities? If so, state how often such assessments are performed and by whom. Yes No
-
- 19.(a) Are wireless communication systems being used to transfer sensitive corporate data? Yes No
- (b) If so, is the data encrypted with at least 64-bit encryption and authenticated? Yes No
- Describe the authentication mechanisms _____
-
- (c) Does the wireless entry point terminate in a DMZ to prevent direct access to your core network?..... Yes No

ARKANSAS: 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.

COLORADO: 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.

DISTRICT OF COLUMBIA: 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.

FLORIDA: 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.

HAWAII: 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: 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.

LOUISIANA: 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.

MAINE: 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.

MINNESOTA: A PERSON WHO SUBMITS AN APPLICATION OR FILES A CLAIM WITH INTENT TO DEFRAUD OR HELPS COMMIT A FRAUD AGAINST AN INSURER IS GUILTY OF A CRIME.

NEW JERSEY: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW MEXICO: 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.

NEW YORK (Non Auto): 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.

OHIO: 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.

OKLAHOMA: 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: Any person who knowingly and with intent to defraud or solicit another to defraud the insurer by submitting an application containing a false statement as to any material fact, may be violating state law.

PENNSYLVANIA: 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 THE PERSON TO CRIMINAL AND CIVIL PENALTIES.

PUERTO RICO FRAUD WARNING: Any person who knowingly and with the intent to defraud, presents false information in an insurance request form, or who presents, helps or has presented a fraudulent claim for the payment of a loss or other benefit, or presents more than one claim for the same damage or loss, will incur a felony, and upon conviction will be penalized for each violation with a fine of no less than five thousand dollars (\$5,000) nor more than ten thousand dollars (\$10,000); or imprisonment for a fixed term of three (3) years, or both penalties. If aggravated circumstances prevail, the fixed established imprisonment may be increased to a maximum of five (5) years; if attenuating circumstances prevail, it may be reduced to a minimum of two (2) years.

TENNESSEE (Non WC): 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.

VERMONT: 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, may be committing a crime, subjecting the person to criminal and civil penalties.

VIRGINIA: 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.

WASHINGTON: 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.

WEST VIRGINIA: 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.

ALL OTHER STATES: 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 civil penalties. Not applicable in Nebraska.

In support of this application for Bond, the undersigned authorized officer of the Financial Institution represents that the statements made herein are true to the best of his/her knowledge, and it is understood the underwriter will rely upon such statements in making its decision to issue or renew any Bond for which this application is made.

Exact Name of Applicant	Officer (Signature & Title)	Date
-------------------------	-----------------------------	------