

COMPUTER FRAUD RIDER

To be attached to and form part of Financial Institution Bond, Standard Form No. 24, No. [policynbr].

It is agreed that:

1. It is agreed that the attached bond is amended by adding the following additional Insuring Agreements:

COMPUTER HACKER INSURING AGREEMENT

Loss resulting directly from an unauthorized party (other than an Employee), acting alone or in collusion with others, entering or changing Electronic Data or Computer Programs within any Computer System or Network:

- (a) operated by the Insured;
- (b) operated by a natural person, partnership or corporation performing services as an electronic data processor of checks or Depositor Services pursuant to a Written contract with the Insured; or
- (c) first used by the Insured during the bond period as provided by General Agreement B of this bond;

provided that the entry or change causes: (1) property to be transferred, paid or delivered, (2) an account of the Insured, or of its customer, to be added, deleted, debited or credited, or (3) an unauthorized account or a fictitious account to be debited or credited.

FUNDS TRANSFER FRAUD INSURING AGREEMENT

Loss resulting directly from an Employee transferring funds from a customer's account by using any Computer System or Network enumerated in (a), (b) or (c) above, while acting in good faith and reliance upon a fraudulent instruction transmitted or received:

- (a) from a software contractor who has a Written agreement with the Insured to design, implement or service programs for a Computer System or Network covered by this Insuring Agreement and where the fraudulent instruction was originated by such software contractor, not by any customer of the Insured, other financial institution, automated clearinghouse or other office of the Insured; or
- (b) through an Electronic/On-Line Communication which communication purports and reasonably appears to have originated from a customer of the Insured, another financial institution, automated clearing house, or another office of the Insured but, in fact, was not originated by the customer or entity whose identification it bears and contains the name of a person authorized to initiate such transfer; or
- (c) by a voice-initiated instruction, which was purported to be from an:
 - (i) individual person who is a customer of the Insured; or
 - (ii) officer, director, partner or employee of a customer of the Insured who was authorized by the customer to instruct the Insured to make such transfer; or

- (iii) Employee of the Insured in another office of the Insured who was authorized by the Insured to instruct other Employees of the Insured to transfer Funds, and was received by an Employee of the Insured specifically designated to receive and act upon such instructions; or
- (d) through a Telefacsimile Device and which instruction purports and reasonably appears to have originated from a customer of the Insured, another financial institution, or another office of the Insured but, in fact, was not originated by the customer or entity whose identification it bears and contains the name of a person authorized to initiate such transfer; or
- (e) through an email and which instruction purports and reasonably appears to have originated from a customer of the Insured, another financial institution, or another office of the Insured but, in fact, was not originated by the customer or entity whose identification it bears and contains the name of a person authorized to initiate such transfer;

provided that with regard to (b):

- (i) the customer is an entity or individual which has a Written Agreement with the Insured authorizing the Insured to transfer Funds from the customer's account to the account of another; and
- (ii) the instruction was verified by a Two-Factor Authentication procedure set forth in the Written Agreement;

and provided that with regard to (c), (d) and (e):

- (i) the customer is an entity or individual which has a Written Agreement with the Insured authorizing the Insured to transfer Funds from the customer's account to the account of another; and
- (ii) if the transfer was in excess of \$25,000, the instruction was verified by an Authentication procedure set forth in the Written Agreement.

COMPUTER VIRUS AND EMPLOYEE SABOTAGE INSURING AGREEMENT

Loss resulting directly from the malicious destruction of, or damage to, Electronic Data or Computer Programs owned by the Insured or for which the Insured is legally liable while stored within a Computer System covered under the terms of the Funds Transfer Fraud Insuring Agreement above, including damage or destruction caused by a Computer Program or similar instruction which was written or altered to incorporate a hidden instruction designed to destroy or damage Electronic Data or Computer Programs in the Computer System in which the Computer Program or instruction so written or so altered is used.

The liability of the Underwriter as to this Insuring Agreement shall be limited to the cost of duplication and/or replacement of such Electronic Data or Computer Programs. In the event, however, that destroyed or damaged Computer Programs cannot be duplicated from other Computer Programs, the Underwriter will pay the cost incurred for computer time, computer programmers, consultants or other technical specialists as is reasonably necessary to restore the Computer Programs to substantially the previous level of operational capability.

Special Conditions and Limitations: For the purpose of this Insuring Agreement only:

- (1) Single Loss shall mean all covered costs incurred by the Insured between the time destruction or damage is discovered and the time the Computer System is restored to substantially the previous level of operational capability. Recurrence of destruction or damage after the Computer System is restored shall constitute a separate Single Loss.
- (2) Exclusion (h) of the bond is deleted in its entirety and replaced with the following: loss caused by an Employee except when covered under Insuring Agreement (A) or this Computer Virus and Employee Sabotage Insuring Agreement.

TOLL FRAUD INSURING AGREEMENT

Loss resulting directly from charges for voice telephone long-distance toll calls which were incurred due to the fraudulent use or fraudulent manipulation of an Account Code or System Password required to obtain access to a Voice Computer System first used by the Insured, installed on the Insured's premises, whose System Administration is performed and controlled by the Insured; provided, however, that the unauthorized access was not made possible by:

- (1) failure to incorporate a System Password feature or failure to change the System Password at least once every 30 days thereafter, or
- (2) failure to have a call-disconnect feature in operation to automatically terminate a caller's access to the Voice Computer System after not more than three unsuccessful attempts to input an Account Code.

2. For the purpose of this rider only, the conditions and limitations contained in the bond shall apply and the following condition and limitation is added:

CONDITIONS AND LIMITATIONS

SERIES OF LOSSES

All loss or series of losses involving the fraudulent acts of one individual (whether or not that individual is identified) or involving fraudulent acts in which a reasonable person would conclude that one individual is implicated, shall be treated as a Single Loss and subject to the Single Loss Limit of Liability. A series of losses involving unidentified individuals, but arising from the identical or substantially similar method of operation shall be deemed to involve the same individual and in that event shall be treated as a Single Loss and subject to the Single Loss Limit of Liability.

3. For the purpose of this rider only, the definitions contained in Conditions and Limitations, Section 1 of the bond, shall apply and the following definitions are added:

DEFINITIONS

- (a) Account code means a confidential and protected string of characters which identifies and authenticates a person and permits that person to gain access to a Voice Computer System for the purpose of making toll calls or utilizing voice mail box messaging capabilities or other similar functional features of the Voice Computer System.

- (b) Authentication means an instruction verification procedure in which the Insured requests and receives confirmation from a customer as to the validity of an instruction the Insured received to transfer Funds, through one of the following communication methods:
- (i) a call back to a Predetermined Telephone Number;
 - (ii) an email to a Predetermined Email Address requiring an affirmative reply; or
 - (iii) a mobile phone application which alerts the customer of the pending transfer request and requires affirmative reply.
- (c) → Computer Program means a set of related electronic instructions which direct the operations and functions of a computer or devices connected to it which enable the computer or devices to receive, process, store or send Electronic Data.
- (d) → Computer System means computers with related peripheral components, including storage components wherever located, systems and applications software, and terminal devices and related communication networks by which Electronic Data are electronically collected, transmitted, processed, stored and retrieved.
- (e) → Confidential Information means any secret, confidential or sensitive information maintained by, and within the control of, the Insured with respect to its own business activities or those of its customers, and where the unauthorized publication of such information would ordinarily constitute a breach of statutory or regulatory law.
- (f) → Depositor Services means establishing, maintaining, administering or servicing an FDIC-insured deposit account.
- (g) → Dual Origination means that two different authorized individuals, at separate terminals or locations, must independently confirm an instruction to transfer Funds via their unique PINs, passwords, or via separate Authentications.
- (h) → Electronic Data means facts or information converted to a form usable in a Computer System or Network by Computer Programs and which is stored on magnetic tapes or disks, or optical storage disks or other bulk media.
- (i) → Electronic/On-Line Communication means a communication that is transmitted through the Insured's Computer System or the Insured's Network and stored electronically on the Insured's Computer System. An Electronic/On-Line Communication does not include a communication delivered through a Telefacsimile Device, via voice or voice recording, or via email.
- (j) → Funds means Money on deposit in an account.
- (k) → Network means a group of Computer Systems that are linked together through communication technology for the purpose of allowing the transfer of information into or out of the Insured's Computer System. Network shall include an automated interbank communication system such as Fedwire, Clearing House Interbank Payment System (CHIPS), or Society for Worldwide Interbank Financial Telecommunication (SWIFT).

- (l) —> Predetermined Email Address means an email address agreed upon by the Insured and customer, other financial institution, automated clearing house, or other office of the Insured as applicable to the transfer at hand, for the purpose of protecting the integrity of a funds transfer instruction received from such customer, other financial institution, automated clearing house, or other office of the Insured by voice, fax, email or an Electronic/On-Line Communication.
- (m) —> Predetermined Telephone Number means a telephone number agreed upon by the Insured and customer, other financial institution, automated clearing house, or other office of the Insured as applicable to the transfer at hand, for the purpose of protecting the integrity of a funds transfer instruction received from such customer, other financial institution, automated clearing house, or other office of the Insured by voice, fax, email or an Electronic/On-Line Communication.
- (n) —> System Administration means the performance of security functions including but not limited to defining authorized persons to access a Voice Computer System and adding, changing and deleting Account Codes or passwords in connection therewith; and invoking or revoking a system option which directs telephone call routing or which adds, moves or drops telephone lines or which performs any other similar activity.
- (o) —> System Maintenance means the performance of hardware and software installation, diagnostics and corrections and similar activities that are performed in the usual custom and practice by a manufacturer or vendor to establish or maintain the basic operational functionality of a Voice Computer System or any component thereof.
- (p) —> System Password means a confidential and protected string of characters which identifies or authenticates a person and permits that person to gain access to a Voice Computer System or any portion thereof for the purpose of performing System Administration or System Maintenance activities.
- (q) —> Telefacsimile Device means a machine capable of sending or receiving a duplicate image of a document by means of electronic impulses transmitted through a telephone line and which reproduces the duplicate image on paper.
- (r) Two-Factor Authentication means:
 - (i) an instruction verification procedure in which the Insured requires the use of a user ID, PIN, or password and a password-generating token or USB token to initiate a request for the transfer of Funds via an Electronic/On-Line Communication; or
 - (ii) Dual Origination; or
 - (iii) any other multi-factor authentication procedure approved by the Underwriter, in writing.
- (s) —> Voice Computer System means a Computer System installed in one location which functions as a private branch exchange (PBX), voice mail processor, automated call attendant or provides a similar capability used for the direction or routing of telephone calls in a voice communications network.

- (t) Written Agreement means a document signed by the customer which:
- (i) authorizes the Insured to rely on instructions received through an Electronic/On-Line Communication, voice-initiated instruction, Telefacsimile Device, or email, as applicable to the transaction(s) at issue, to make transfers from that customer's account to another account;
 - (ii) has provided the Insured with the names of persons authorized to initiate such transfers and the transfer at issue was purportedly initiated by an authorized person; and
 - (iii) establishes the instruction verification mechanism to be used by the Insured for all such transfers.

4. For the purpose of this rider only, all exclusions contained in Conditions and Limitations, Section 2 of the bond, shall apply. In addition, the following exclusions are added:

EXCLUSIONS

- (a) Loss resulting directly or indirectly from the assumption of liability by the Insured by contract unless the liability arises from a loss covered by this rider and which would be imposed on the Insured regardless of the existence of the contract;
- (b) Loss resulting directly or indirectly from negotiable instruments, securities, documents or other Written instruments, exclusive of any instruction set forth in paragraphs (a) through (e) of the Funds Transfer Fraud Insuring Agreement above, which bear a forged signature, or are counterfeit, altered or otherwise fraudulent and which are used as source documentation in the preparation of Electronic Data or manually keyed into a data terminal;
- (c) Loss resulting directly or indirectly from:
 - (1) mechanical failure, faulty construction, error in design, latent defect, fire, wear or tear, gradual deterioration, electrical disturbance or electrical surge which affects a Computer System or Network, or
 - (2) failure or breakdown of electronic data processing media, or
 - (3) error or omission in programming or processing,
 unless such loss is covered under the Computer Virus and Employee Sabotage Insuring Agreement above;
- (d) Loss to a customer's account resulting directly or indirectly from the input of Electronic Data into a Computer System or Network by a person who had authorized access to the customer's authentication mechanism;
- (e) Loss resulting directly or indirectly from the theft of Confidential Information, except when such theft results directly in an account of the Insured or its customer being debited or deleted;
- (f) Loss resulting directly or indirectly from the fraud or dishonesty of a natural person, partnership or corporation performing Depositor Services or services as a data processor of checks or from the fraud or dishonesty of the partners, officers, or employees of such natural person, partnership or corporation.

5. The Single Loss Limit of Liability and the Single Loss Deductible for the **COMPUTER FRAUD RIDER** are the amounts shown on the Declarations Page or amendment thereto. The Single Loss Limit of Liability under this Rider shall be a part of, and not in addition to, the amount stated in Item 4 of the Declarations.
6. This rider shall be effective as of 12:01 a.m. on [endorsementeffdt].

Nothing herein contained shall be held to vary, alter, waive or extend any of the terms, conditions, provisions, agreements or limitations of the bond, other than as above stated.

SPECIMEN