The Surety & Fidelity Association of America ("SFAA") submits for filing the Computer Crime Policy for Financial Institutions TSB 6189a. In addition, SFAA files the enclosed application Computer Crime Policy for Financial Institutions SA 6192a.

SFAA is revising its Computer Crime Policy for Financial Institutions ("Policy"). The evolving nature and use of computers and technology have mandated that substantial revisions be made to the Policy, which was drafted initially in the 1980s.

The Policy offers four insuring agreements:

1. Computer to Computer Systems Fraud – Access Credentials. This insuring agreement covers loss caused by a computer generated transfer (with no human intervention) caused by unauthorized access using misappropriated access credentials. This insuring agreement actually is divided into two parts: one for consumer accounts and the other for commercial accounts.
2. Computer to Computer Systems Fraud – Hacker or Interloper. This insuring agreement covers loss caused by a computer generated transfer (with no human intervention) caused by hacking.
3. Fraudulent Transfer Instructions.
4. Fraudulently Induced Transfer. This insuring agreement covers loss caused by a wire transfer by which the insured's employee was induced fraudulently to make such a transfer.

As a general matter, the Policy contemplates that both the financial institution and the institution's customer have employed reasonable security practices and controls, and the perpetrator defeated those controls. The Policy contemplates the risk apportionment provisions in the Uniform Commercial Code.

The following are comments regarding specific provisions in the Policy:

Computer to Computer Systems Fraud – Access Credentials

- This insuring agreement covers the loss of certain types of property directly caused by an unauthorized access and transfer, through an account takeover with misappropriated access credentials.
- Because the liability rules differ between a consumer account and a commercial account, the Computer to Computer Systems Fraud insuring agreement is divided into two parts with a separate limit of insurance and deductible for each.
- The language "with no action, authorization or intervention by an Employee" emphasizes that the transaction contemplated is entirely automated. A transaction in which the insured's employee must act to effect the transfer would be addressed by the Fraudulent Transfer Instructions Insuring Agreement or the Fraudulently Induced Transfer Insuring Agreement.

Computer to Computer Systems Fraud – Hacking

- This insuring agreement covers the loss of certain types of property directly caused by an unauthorized access and transfer, through hacking. The transfer is entirely automated with no human intervention.

Fraudulent Transfer Instructions

- This insuring agreement covers the loss of certain types of property directly caused by a transfer that was initiated or authorized by an employee on the good faith reliance on fraudulent instructions sent via telephone, fax, email or online banking system.
- To emphasize that there must be a human actor to cause the transfer, the draft includes the explicit involvement of an employee of the insured.
- This coverage includes the institution's "online banking system" as another means by which instructions are sent.
- This coverage specifies that any other verification procedure that is used must be "out of band".

Fraudulently Induced Transfers

- The Policy includes coverage for fraudulently induced transfers related to vendor or employee impersonations. The coverage does not extend to customer impersonations, as this particular scenario (i.e. the fraudster impersonates a customer who provides wire instructions to the bank) likely would fall under Fraudulent Transfer Instructions coverage. In recent years, businesses, including financial institutions, have experienced a fraudulent scheme that was not contemplated under the Fraudulent Transfer Instructions Insuring Agreement. In particular, the fraudster impersonates a vendor or employee of the insured and contacts the insured requesting a wire transfer of funds. Then, based on this phony information, a legitimate employee of effects the wire transfer based on the phony information. Thus, intended to send to the payment. However, the employee was induced fraudulently making the payment. The exposure for such scams can be significant. According to the Federal Bureau of Investigation Internet Crime Complaint Center, between October 2013 and December 2014, such scams resulted in losses totaling $214,972,503.30.[1]

General Agreements

- All General Agreements generally are the same as the provisions in the Financial Institution Bond, except the Consolidation General Agreement. The version in the Policy references the acquisition of Computers.

[1] Brian Donohue, *FBI:Business Email Compromise Scams Steal $214M in 2014*, Threatpost, January 28, 2015 (available at https://threatpost.com/fbi-business-email-compromise-scams-steal-214m-in-2014/110715).

Definitions

- Computer is defined broadly and is intended to include smart phones.
- "Insured's Computer" is used rather than "Computer System" (as used in the current Computer Crime Policy). The definition includes computers that are maintained by a third party service provider.
- Cryptocurrency, which is excluded, is a defined term.
- The definition of Customer has been simplified to mean only a person that has a written agreement with the insured. The contents of the agreement are set forth in a Condition.
- Commercial Accounts and Consumer Accounts are distinguished in the definitions.
- The definition of Employee is not as broad as the definition in the Financial Institution Bond because it is an Employee that effects wire transfers, and the population of persons that may make wire transfers should be constrained.
- The definition of Network includes the Internet.
- Payment Order is similar to the definition in the Uniform Commercial Code.

Exclusions

- The exclusions are similar to those in the current Computer Crime Policy.
- Of special note:
    - Exclusion (s) excludes loss involving cryptocurrency.
    - Exclusion (t) is intended to exclude coverage for a loss incurred by the bank in cases where the bank, by law or contract, should not have borne the loss but paid the customer simply in the interest of customer relations.
- The former Exclusion (p) in the prior Computer Crime Policy referred to telegraphic and cable instructions and an exception for "Tested" instructions. These these terms and the exclusion were outdated. The exclusion was deleted.

Conditions

- Generally, the conditions are incorporated from the Financial Instituon Bond.
- The Covered Property condition is specific to the property involved in computer crime transactions.
- The Policy includes three conditions precedent.
    - Condition 12 requires the insured to pursue claims or defenses with the Customer.
    - Condition 13 requires the insured to be in compliance with established security procedures, with respect to an Insuring Agreement 1 loss involving a commercial account.
    - Condition 15 requires the insured to verify the identity of the vendor or employee before ordering the transfer of funds under Insuring Agreement 4.
- The Single Loss Condition refers to losses involving the same method of operation. In order to foreclose "connecting" losses simply because they use the same method of operation, "related" modifies losses.

- The insured is required to include certain provisions in the customer agreement, as a condition of the Policy (Condition 14).
- Condition 17 incorporates the provision from the Data Breach Exclusion rider (SR 6322).