The increasing usage of sophisticated computer and payments systems by financial institutions has created new and complicated exposures to criminal loss. Funds-transfer and computer activities represent exposures to fraud and theft by employees, customers, service contractors and many others. Fortunately losses in this category - not covered by the various Bankers’ Blanket Bonds have not been significant to date. The potential for a huge increase in such losses, however, is certainly present.

Increased reliance on automated systems has led both bankers and insurers to re-examine insurance coverage. They found that while the BBB would cover losses associated with employee fraud in the bank’s automated systems, it did not cover fraud perpetrated by third parties using telecommunications links connected to the computer systems.

Underwriters at Lloyd’s were the first to design a policy to cover the risks associated with the use of computers and modern telecommunications systems by financial institutions. Similar coverage is now offered by US insurers and takes the form of either a separate policy or a “rider” to the BBB.

An Electronic and Computer Crime Policy consists of the following vital components:

- **COMPUTER SYSTEMS**

  Coverage in respect of losses sustained through acting upon data which has fraudulently been input on the computer system or fraudulently modified. Intended for the coverage of electronic or computer use in the following areas:

  - The Insured’s own computer systems.
  - A Customer Communication system.
  - A Service Bureau’s Computer system.
  - Electronic funds transfer system.

  Coverage in respect of losses sustained through fraudulent destruction of electronic data Stored or being run through any one of the above systems or during transmission to the Assured’s computer system or Service Bureau’s system.

  Fraudulent input of data through a Telephone Banking system into the Assured’s system.
• **ELECTRONIC COMPUTER PROGRAMS**

Protection for losses arising from electronic instructions which have either been fraudulently prepared or fraudulently modified.

• **ELECTRONIC DATA AND MEDIA**

This section of coverage offers protection against risks of physical loss or damage to electronic data process media, similar to the “Premises” and “Transit” clauses of the BBB. Providing the assured with coverage in respect of the malicious alteration or destruction of electronic data processing media (discs, magnetic tapes or any other media on which data may be stored) while on the premises of the Assured or while in transit.

• **COMPUTER VIRUS COVER**

Coverage is provided for the transfer of funds or property as a direct result of the destruction or attempt thereat of the Assured’s electronic data due to a computer virus. Coverage is provided for destruction or attempt of threat to the Assured’s electronic data as a result of a computer virus caused by any person.

• **ELECTRONIC AND TEFACSIMILE COMMUNICATIONS**

Protection against financial loss sustained as a result of the assured acting upon certain types of funds transfer instructions, which have been altered in transmission or which purport to have come from a customer, Automated Clearing House or another financial institution, but in fact do not.

Means of transmission: a) Electronic Communications System
b) by tested telefacsimile, telex or similar

• **ELECTRONIC AND TELEFACSIMILE COMMUNICATIONS**

Coverage is provided for fraudulent electronic communications received from:
- Electronic Communication System

Tested communication [as detailed in the insuring clause]

Which purports to have been sent by a customer, Automated clearing house, etc.
• **ELECTRONIC TRANSMISSIONS**

Legal liability protection for losses to customers, Automated Clearing House or another financial institution arising from electronic instructions [communication systems detailed in Insuring clause] which were alleged to be sent by the assured but which were not, or were fraudulently altered during transit or electronic transmission.

The legal liability arising from the Assured’s responsibility as a Service Bureau to a customer, Automatic clearing house or financial Institution as a direct result of the fraudulent input, modification, destruction of Electronic Data stored on the Assured’s computer system.

• **ELECTRONIC SECURITIES**

Legal liability coverage in respect of loss incurred by a Central Depository when the institution has acted upon electronic instructions which purportedly were believed to have been sent by the insured and which in practice were not, or were modified fraudulently during physical transit. Means of transmission: a) Electronic Communications System
c) by tested telefacsimile, telex or similar means of communication

• **FORGED TELEFACSIMILE**

A very large proportion of instructions initiating EFT payments enter financial institutions via the telephone or facsimile message, underlining the importance of this form of coverage. Protection is provided in respect of losses sustained due to the fraudulent transmission of facsimile messages, purporting to have come from a customer, another office of the insured or from another financial institution, being sent without permission and a forged signature.

• **VOICE-INITIATED TRANSFERS**

Protection for voice initiated funds transfer instructions. It should be noted that Underwriters will require that a structure of specific minimum standards are in place with regard to procedure before providing coverage in this respect.

Customers’ agreement shall be in the form of a corporate resolution containing a list of individuals authorised to initiate and authenticate voice initiated funds transfers, which list must specify the telephone numbers as well as monetary limits for all initiators/authenticators. Such written agreement shall also outline the terms and conditions under which the service is provided including a limitation of liability accepted by the Assured.

**SPECIAL CONDITION**

All voice initiated instructions purportedly received from a customer for the transfer of funds or property must be Tested or subject to a call-back to an authorised person other than the individual initiating the transfer request.
EXTENSIONS TO COVERAGE:

*Definition E amended to include personal computers.*
This clause extends the definition of computer systems to include personal computers.

*Establishment of a Clean Up Costs Extension*
This extension to coverage provides for the verification and reconstitution of electronic computer instructions which have been fraudulently prepared/modified so as to give rise to a loss under the computer crime section of the policy.

*Letter of intent in respect of Exclusion “O”*
This clause clarifies the intention of this exclusion to avoid any dispute in the event of a loss.

*Insuring Clauses 6 and 7 (Communications and Transmission)*
Are amended to include communications recorded on Electronic Data or Electronic Data Processing Media.

*Exclusion(s) is amended by the addition of the words “...unless discovered within 60 days of such acquisition when covered under Insuring Clause 3”.*