Summary of Market Clarifications

In September 2012, an appellate court upheld a judgment against AIG requiring payment of over $7 million for a computer hacking insurance claim (Retail Ventures Inc. et al. v. National Union Fire Insurance of Pittsburgh, Pa., case number 10-4576, August 23, 2012.). The policyholder, a nationwide retailer, filed its claim after hackers stole credit card and checking account information for over 1 million customer account transactions, which resulted in fraudulent credit card charges, credit monitoring costs, re-establishment of accounts, call center costs, legal expenses, and a spate of class action suits, as well as an inquiry by the FTC. The decision rejected AIG’s attempt to exclude coverage on the grounds that the "direct loss" provision in its crime insurance policy excluded the computer hacking claim. The decision instead found that coverage existed for the losses suffered by the retailer for, among other things, reimbursing others for fraudulent credit card charges and expenses for addressing an FTC inquiry (as reported at andersonkill.com/news_article.asp?newsid=1236).

Very soon after this court ruling, the Crime marketplace went to work clarifying their policies were never intended to be a Cyber policy. Today we see exclusions for:

- Disclosure of an insured’s or another entity or person’s confidential or personal information while in the care, custody or control of an insured including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any similar type of nonpublic information.

- Fees, costs, fines, penalties or any other expenses incurred by an insured which result from the access to or disclosure of another entity or person’s confidential or personal information.

- Expenses related to your obligations to comply with federal and state privacy laws and Payment Card Industry Data Security Standards arising from a data security breach.

Some carriers have even gone a step further to exclude claims if the insured fails to follow security procedures:

- Loss resulting from your failure to follow security procedures agreed to in writing with your customer or your financial institution.

- Loss that would have been avoided if you had accepted and followed commercially reasonable security procedures that your financial institution made available for your account or accounts involved in the loss; or

- Loss resulting from your failure to comply with security procedures that you represented you would follow.

(Security procedure is defined as a procedure established by agreement of the insured and its customer or financial institution for the purpose of (i) verifying that a payment order is that of the insured, or (ii) detecting error in the transmission of the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.)

(Continued on back)
What Coverage Is Available Under a Crime Policy?

**Computer Fraud** – loss of money, securities, and other property directly caused by a third party/non employee via Computer Fraud. Computer Fraud is the use of any computer to fraudulently cause a transfer of money, securities or other property from the premises of the insured or a financial institution premises to a person or place outside the premises of the insured or financial institution premises.

**Computer Program and Electronic Data Restoration Expense** – reasonable restoration expense that the insured incurs to restore or replace damaged or destroyed computer programs or electronic data stored within the insured’s computer system directly caused by a computer violation. Computer violation means a computer virus designed to damage or destroy a computer program or electronic data or vandalism by a natural person who has gained unauthorized electronic access to the insured’s computer system. This coverage is normally sublimited to less than $500,000 and not available with all carriers.

**Funds Transfer Fraud** – loss of money and securities contained in the insured’s transfer account directly caused by a third party/non employee via Funds Transfer Fraud. Funds Transfer Fraud means:

- Electronic, telegraphic, cable, teletype, or telephone fraudulently transmitted to a financial institution directing such institution to debit a transfer account and to transfer, pay or deliver money or securities from the transfer account which instruction purports to have been transmitted by the insured, but was in fact fraudulently transmitted by someone other than the insured without the insured’s knowledge or consent;

- Fraudulent written instruction, other than one covered under Forgery or Alteration, issued to a financial institution directing such financial institution to debit a transfer account and to transfer, pay or deliver money or securities from such transfer account by use of an electronic funds transfer system at specific intervals or under specified conditions, which written instruction purports to have been issued by the insured but was in fact fraudulently issued, forged or altered by someone other than the insured without the insured’s knowledge or consent; or

- Electronic, telegraphic, cable, teletype, telefacsimile, telephone or written instruction initially received by the insured, which purports to have been transmitted by an employee, but which was in fact fraudulently transmitted by someone else without the insured’s or the employee’s consent.

---

**SPECIAL REPORT: CYBER & CRIME**

Revenues a typical organization loses to fraud each year.

$145,000
Median loss from single case of occupational fraud.

22%
Occupational fraud cases with losses of $1 million +.

28%
Higher median fraud losses for organizations with fewer than 100 employees.

$80,000
Median loss to fraud (single perpetrator)

$300,000
Median loss to fraud (multiple perpetrators)

All data drawn from ACFE.com