

Fidelity Bond And Commercial Crime Coverage For Computer Fraud Claims

Given the headlines in recent months regarding massive computer security breaches, insurance coverage concerns for corporate policyholders have never been greater. With the insurance market for computer-related perils in an absolute state of disarray, and the products being sold in a state of constant flux, policyholders face significant challenges in protecting against computer hacking perils in ways that simply were not of much concern just a few years ago. Now that businesses of all stripes are almost entirely computer system dependent for even the most routine business tasks and recordkeeping, information on almost every facet of an organization's operations is maintained on computer networks, laptop computers, and off-site servers, as well as on back-up computers.

Computer hacking attacks have been staggering recently in terms of their sheer magnitude. One computer hacking incident resulted in either 40 million or 100 million customer transactions stolen by the hacker (depending upon which account one believes). Not only was the number of personal account transaction records stolen unreal, but so too were the costs to the policyholder

in responding to this misfortune. As such, it is important for policyholders to understand what insurance coverage they may have to protect against such perils. Coverage may be available to defray the significant costs of a serious hacking attack, but recovering that insurance protection is almost never easy.



JOSHUA GOLD

Array Of Losses

Compounding the problem, a sophisticated hacker can access all manner of information, including health records, employment records, credit card account numbers, security codes, checking account numbers, Social Security numbers, driver license numbers and other business, employee and personal information, just to name some of the categories of information that is captured electronically. When these types of information are hacked, policyholders often suffer an array of losses, including business interruption loss, theft loss, class action lawsuits and costs attendant to notifying customers and clients of the hacking incident. A number of insurance policies may provide insurance coverage for such misfortune, including property insurance, business income coverage, business liability insurance, fidelity bonds, comput-

er crime policies, inland marine insurance policies and other forms of insurance coverage.

Commercial crime insurance policies and fidelity bonds with so-called "computer fraud" riders promising coverage for security breaches caused by computer hackers may prove especially handy. One form of crime insurance coverage promises protection for "loss or damage to money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises." Another insuring provision under a crime form promises protection for "loss of and loss from damage to Covered Property resulting directly from the Covered Cause of Loss," where Covered Property is defined to mean "Money, Securities and Property other than Money and Securities." Covered Cause of Loss is defined to mean "Computer Fraud."

Insurance Company Excuses

Despite these seemingly broad promises of protection, insurance companies are known to assert numerous excuses to bar or reduce coverage at the time a computer fraud claim is filed. As such, policyholders have to be on guard for the numerous rationales insurance companies offer to avoid

their coverage obligations for computer-related theft claims.

One such defense to coverage is that the information hacked was either “records,” “confidential information,” “trade secrets,” “manuscripts” or “drawings.” The insurance company may argue that “loss” resulting from such information is subject to a sub-limit of coverage or is excluded altogether. Many fidelity and crime insurance policies, however, fail to provide complete or clear definitions of the terms used to establish the rights and obligations of the parties. This fact alone may give policyholders the advantage since more than 99 percent of all insurance policies are contracts of adhesion, requiring that any uncertain or ambiguous policy language be interpreted in the policyholder’s favor and against the insurance company. It is not surprising then that insurance companies are trying to strip these legal protections by adding arbitration clauses and modified choice of law provisions to some of their insurance products.

A second popular defense to insurance coverage raised by fidelity and commercial crime insurance companies is that there is no or only limited insurance coverage for third-party claims. Here, the insurance company argues that its insurance policy only covers so-called “direct loss” and that any claim involving injury to or legal action by a third-party “never” constitutes “direct loss.” In this situation, policyholders are wise to check the law and check their policy terms to ensure that they are not getting a false bill of goods from their insurance company. As a preliminary matter, many fidelity bonds and commercial crime insurance policies do pro-

vide protection for an array of third party claims—offering both coverage for compensatory damages and even legal fees in some instances. Moreover, numerous courts around the country have rejected insurance company attempts to improperly narrow the coverage promised to policyholders under fidelity and commercial crime policies. Specifically, many of these judicial decisions have ruled that the “direct loss” defense is not the stringent, coverage defeating clause that insurance companies urge at claims time. It is also revealing that this coverage “defense” is never discussed or highlighted for policyholders at the point of purchase during underwriting and broker meetings or during policy renewals.

In The Courts

Thus far, there are very few court decisions that discuss or spell out the scope of insurance coverage for computer fraud incidents. Accordingly, many of the vaguely defined terms and pressure points of the more popular fidelity and computer crime insurance policy forms remain judicially un-tested and un-interpreted. One interesting United Kingdom case from a couple of years ago did explore insurance coverage under a policyholder’s insurance policy that covered property and theft losses. There, the policyholder lost valuable source code due to a computer virus and the theft of a computer in two separate incidents. The insurance company sought to avoid payment of the insurance claim and litigation ensued. The insurance company argued against coverage by claiming that a “malicious persons” exclusion barred coverage for any claims of theft of the

source code. The UK appellate court rejected this argument and held that there was insurance coverage for the virus and the computer theft and that “if the insurer wished to exclude all damage caused, however indirectly, by a computer hacker, [it] needed to place that exclusion in a separate clause.”

It is very likely that decisions from the U.S. regarding claims of computer fraud will start showing up soon as policyholders that suffer massive computer hacking attacks seek to implicate insurance coverage under crime and fidelity policies promising computer fraud protection. Given the size of these claims and the (now) recurring nature of such claims, one can expect the insurance industry to heavily scrutinize these claims and, in many instances, to fight them all the way to the courthouse steps.

Joshua Gold is a shareholder in the New York office of the law firm of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders in insurance coverage matters and disputes concerning time element insurance, electronic data and other property insurance coverage issues. Mr. Gold can be reached at jgold@andersonkill.com or (212) 278-1886.

