Computer crime covers for third-party loss? Only in Ohio

As businesses have become increasingly dependent upon computers, the insurance industry has been called upon to offer new products to protect against the attendant risks. Fidelity insurers were among the first to respond with the development of computer crime coverage. Unlike specialised cyber liability policies, however, computer crime coverage contains a key feature present in almost all fidelity coverages, ie, coverage is available only for losses resulting directly from the covered peril – here, computer fraud. By contrast, more recently-developed cyber liability policies offer coverage for third-party liability. In *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, PA, 2012 WL 3608432* (6th Cir. 2012), the US Court of Appeals for the Sixth Circuit blurred the distinction between computer crime and cyber liability policies by holding that computer crime coverage afforded coverage for an insured's third-party liability.

The insured in *Retail Ventures* was the victim of a computer hacking scheme by which hackers gained unauthorised access to the insured's main computer system and downloaded credit card and checking account information on the insured's customers. The hackers then used the information to conduct fraudulent transactions. Thereafter, the insured incurred expenses arising from resulting customer claims and lawsuits, investigations by seven state attorneys general and the Federal Trade Commission, customer communications, and public relations.

The insured sought coverage for its losses under a blanket crime policy issued by National Union. The policy contained computer and funds transfer coverage, under which National Union agreed to pay the insured for "[l]oss which the insured shall sustain resulting directly from . . . The theft of any insured property by computer fraud." The policy's definition of computer fraud included "the wrongful conversion of assets under the direct or indirect control of a computer system by means of . . . [t]he fraudulent accessing of such computer system."

National Union did not dispute that computer fraud had occurred. It declined coverage, however, on the basis that, *inter alia*, the insured's losses did not result directly from computer fraud. Rather, National Union took the position that the direct cause of the losses was the insured's legal liability to third parties who asserted claims after the data breach had occurred. In other words, National Union's position was that computer fraud was the indirect cause, not the direct cause, of the insured's losses.

Although no Ohio state or federal court had previously considered whether fidelity bonds afforded coverage for third-party liability, National Union urged the court to follow the position, adopted by a majority of courts, that the "resulting directly from" language requires that the theft be the "sole" and "immediate" cause of the insured's loss. The Sixth Circuit declined to do so, opting instead to look to a few Ohio cases in which the court applied a proximate cause standard to determine whether a "direct" loss had occurred under a property policy and a windstorm policy. Relying on those cases, the Sixth Circuit predicted that the Ohio Supreme Court would apply the broader proximate cause standard and, on that basis, concluded that the insured's loss resulted directly from the theft of insured property by computer fraud.

The *Retail Ventures* holding potentially opens a Pandora's Box of computer coverage for third-party liability that was never contemplated by fidelity insurers. Some commentators have even suggested that, because of the decision, insurers now should look to their fidelity bonds for broader cyber coverage. This conclusion is at odds with the history of computer crime coverage, which has not been held to cover third-party liability. Moreover, this position ignores the insurance industry's response to the rise in cyber exposures. Insurers and brokers have not been touting computer crime coverage as the answer to companies' evolving cyber risks. (Some broker literature even cautions that computer crime coverage does not cover third-party liability.) Instead, for the past several years, the industry has been hard at work in developing and marketing a host of cyber liability policies to address the very types of losses not covered by computer crime policies. Such policies include coverage for a variety of risks including legal liability to others for computer security and privacy breaches, legal liability for online media content, costs associated with regulatory investigations and proceedings, and customer notification costs.

In today's marketplace, companies have numerous options for combating cyber liability to third-parties. Until the issuance of R*etail Ventures*, the traditional computer crime coverage has not been one of them. For the moment, however, that is only the case in Ohio. ●

This article is by Bill Lutz, a partner in Clyde & Co's San Francisco office. The decision in Retail Ventures was discussed at the Financial Institutions Conference hosted by Clyde & Co's international financial lines team in London on October 9 2012

The US Court of Appeals for the Sixth Circuit blurred the distinction between computer crime and cyber liability policies by holding that computer crime coverage afforded coverage for an insured's third-party liability.