The Coverage Inkwell

Emerging Coverage Issues in Intellectual Property, Privacy, and Cyber Liability

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

September 11, 2012

DATA BREACH ALERT: COPIED CUSTOMER INFORMATION IS LOSS, BUT NOT "CONFIDENTIAL INFORMATION" UNDER EXCLUSION

Cyber attacks are potentially the biggest risk to security the country faces, according to Homeland Security Secretary Janet Napolitano. Napolitano was here in Philadelphia yesterday, addressing the American Society for Industrial Security. Cyber attacks also constitute a heck of an insured risk.

Data breaches are expensive for everyone. They are expensive for retailers whose computer systems are hacked and information is stolen, and they can be expensive for the consumers whose information is compromised. Data breaches also can be expensive for insurers. The footwear retailer DSW suffered losses in the millions—including over $4 million in costs associated with charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard. And, we haven't even begun to talk about class actions.

In *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, PA*, -- F.3d --, 2012 WL 3608432 (6th Cir. Aug. 23, 2012), the Sixth Circuit recently addressed two frequent coverage issues implicated by data breach claims and the application of the policy exclusion for loss of trade secrets and confidential information. The Court of Appeals rightly concluded that theft and unauthorized copying of information from computer hacking constitutes a "loss." In doing so, the court debunked the antiquated requirement that a "loss" must involve the destruction of information—a concept utterly contradictory with intellectual property infringement and computer fraud. However, the court still refused to apply the exclusion, and, in doing so, misused the principle *ejusdem generis* to limit the broad phrase "confidential information of any kind" found in the exclusion. That is unfortunate, because other courts—when examining similar language—could choose to follow the Sixth Circuit's path. The facts of the case are as follows:

In a span of just 14 days in February of 2005, computer hackers used the local wireless network at a single DSW Shoe Warehouse store to access DSW's main computer system and download credit card and checking account information pertaining to more than 1.4 million customers of

108 stores. *Retail Ventures*, 2012 WL 3608432 at *1. (This fact highlights just how efficient and devastating computer hacking can be.) The stolen information included the magnetic stripe on the back of customer credit cards, customer bank accounts, and driver's licenses. *Id.* Fraudulent transactions using the stolen information followed, and DSW was alerted by credit card companies of the transactions in early March 2005. DSW investigated and uncovered the data breach, and promptly alerted National Union. *Id.* Expenses followed in the form of public relations, customer claims and lawsuits, and attorney fees incurred in connection with investigations by 7 state Attorneys General and the Federal Trade Commission. *Id.*

National Union issued a "Blanket Crime Policy," which included an endorsement entitled "Computer & Funds Transfer Fraud Coverage" that provided coverage for "Loss which the Insured shall sustain resulting directly from : A. The theft of any Insured property by Computer Fraud[.]" *Id.*, *4. The endorsement defined "Computer Fraud" as:

> the wrongful conversion of assets under the direct or indirect control of a Computer System by means of: (1) The fraudulent accessing of such Computer System; (2) The insertion of fraudulent data or instructions into such Computer System; or (3) The fraudulent alteration of data, programs, or routines in such Computer System.

Id. (emphasis added).

"Insured property" was defined as:

> The Insured property may be owned by the Insured, or held by the Insured in any capacity whether or not the Insured is liable for the loss thereof, or may be property as respects which the Insured is legally liable; provided, Insuring Agreements II, III and IV apply only to the interest of the Insured in such property,....

The endorsement also specified that coverage thereunder applied "only with respect to ... Money or Securities or Property located on the premises of the Insured." *Id.*

National Union contended there was no coverage. It did not dispute that the unauthorized access and copying of customer information from DSW's computer system involved the "theft of any Insured Property by Computer Fraud." Instead, it contended that DSW's loss did not result "directly from" the theft of any insured property by Computer Fraud. It also contended that any such loss also was barred by a trade secret/confidential information exclusion in the policy. The district court disagreed and the Sixth Circuit affirmed.

"Resulting directly from" imposes a proximate cause standard. Preliminarily, and as an issue of first impression, the district court concluded that DSW's loss was covered, concluding that the Ohio Supreme Court would follow those cases that interpret the phrase "resulting directly from" to impose a traditional proximate cause standard. Here, the district court concluded that "there is a sufficient link between the computer hacker's infiltration of [DSW's] computer system and [DSW's] financial loss to require coverage under Endorsement 17." *Id.* On appeal, National Union contended that the phrase "resulting directly from" implicated a

heightened standard requiring that the theft of property by computer fraud be the "sole" and "immediate" cause of the DSW's loss. *Id.*, *5. The Sixth Circuit disagreed:

> Despite defendant's arguments to the contrary, we find that the phrase "resulting directly from" does not unambiguously limit coverage to loss resulting "solely" or "immediately" from the theft itself. In fact, Endorsement 17 provided coverage for loss that the insured sustained "resulting directly from" the "theft of any Insured property by Computer Fraud," which includes the "wrongful conversion of assets under the direct or indirect control of a Computer System by means of ... fraudulent accessing of such Computer System."

Id., *8

The Trade Secret/Confidential Information Exclusion did not apply. National Union also contended that coverage was excluded by a trade secret/confidential information exclusion in the policy endorsement, which provided that:

> Coverage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind.

Id., *9. At issue was (1) whether an unauthorized copying of information constituted a "loss" and (2) was it a loss of proprietary information, trade secrets, or "other confidential information of any kind." The Sixth Circuit held that the unauthorized copying did constitute "loss," but not a loss of confidential information of any kind.

The district court held that the term "loss" was ambiguous because it could mean the destruction or deprivation of material, which was not the same as an unauthorized copying of the information. The Sixth Circuit did not agree with this extreme conclusion, and that was the right call. Looking to dictionary definitions for the word "loss," the Sixth Circuit agreed that the term's meaning included loss by destruction or possession, but concluded that this meaning did not make the term ambiguous. Rejecting the argument that "any loss" cannot include fraudulent accessing and copying of information without removing or destroying the data, the Sixth Circuit explained "the plain and ordinary meaning of 'any loss' encompasses the 'theft' of such data even if it is not destroyed or rendered inaccessible in the process." *Id.*, *9.

The Sixth Circuit, however, agreed with the district court that the underlying data breach claim did not involve the loss of proprietary information, Trade Secrets, or other confidential information of any kind. Id., *10. The basis of its conclusion was that DSW did *not own* the information that was stolen because, ultimately, the information belonged to customers and other entities:

> Examining the exclusion for its plain and ordinary meaning, the district court concluded that loss of proprietary information would mean the loss of information "to which Plaintiffs own or hold single or sole right." *In fact, as the district court found, the stolen*

> *customer information was not "proprietary information" at all, since the information is owned or held by many, including the customer, the financial institution, and the merchants to whom the information is provided in the ordinary stream of commerce.* The district court did not err in finding that the stored data consisting of customer credit card and checking account information would not come within the plain and ordinary meaning of "proprietary information."

Id. (emphasis added).

The Sixth Circuit also rejected that the customer information came within the exclusion's broad "catch-all" clause excluding coverage for "loss of ... confidential information of any kind," relying on the construction canon of *ejusdem generis,* in which a general term takes its meaning from the specific terms with which it appears. Here, the court identified those specific terms as "Trade Secrets" and "Confidential Processing Methods," both of which appear in the exclusion's language. Id.

Looking to the common law definition of "trade secrets," and dictionary definitions for "confidential" "processing" and "method," the Sixth Circuit held that the terms limited the meaning of "confidential information of any kind" to prevent application of the exclusion to the data breach claim.

> The district court did not err in finding that "proprietary information," "Trade Secrets," and "Confidential Processing Methods," are specific terms that all pertain to secret information of plaintiffs involving the manner in which the business is operated. The last item, "other confidential information of any kind," is most certainly general and should be interpreted as part of the sequence to refer to "other secret information of *Plaintiffs* which involves the manner in which the business is operated." The "stolen" customer information was not plaintiffs' confidential information, but was obtained from customers in order to receive payment, and did not involve the manner in which the business is operated.

Id., *11.

The court rightly concluded that theft of information constitutes "loss." The requirement that "loss" must involve the removal or destruction of information is antiquated and utterly contradictory with concepts of intellectual property infringement, hacking, and computer fraud. However, the court got it wrong when refusing to apply the exclusion.

The court misused the principle *ejusdem generis* to limit the broad phrase "confidential information of any kind." A quick examination of Black's Law Dictionary reveals that *ejusdem generis* is the principle whereby the meaning of a general phase is limited *if followed by* an enumeration of more specific terms. The phrase "confidential information of any kind" came at

the end of the exclusion and *was not followed by* any specific terms. One can only assume the placement of the phrase at the very end of the exclusion's language was intentionally done by underwriters to avoid the effect of *ejusdem generis.*

The effect of the court's decision is to broaden the risk, contradicting the intentions of the contracting parties, thereby giving away coverage never paid for. That is regrettable. Let's hope other courts similarly do not misuse *ejusdem generis* to find coverage.

Questions are welcome.

The Coverage Inkwell

Joshua A. Mooney | Counsel
1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103-7395
Direct 215.864.6345 | Fax 215.399.9613
mooneyj@whiteandwilliams.com | whiteandwilliams.com
Assistant: Dana Genovese | 215.864-6331

White and Williams LLP