



The Sixth Circuit Weighs in on the “Direct Loss” Issue for Cyber Fraud Coverage

by Geoffrey Miller and Andrew Heckler*

Earlier this month, [SDV reported on a recent Second Circuit case where the court broadly interpreted the “direct loss” requirement to find coverage for a cyber fraud, email spoofing scam](#). Now, the Sixth Circuit Court of Appeals has issued a similar opinion in [American Tooling Center, Inc. v. Travelers Casualty & Surety Company](#), finding coverage for a company that lost \$834,000 to a similar scam. These recent decisions may indicate a trend in favor of policyholders on the “direct loss” issue.

The Fraud and Insurance Claim

The plaintiff, American Tooling Center, Inc. (“American Tooling”), a tool and die manufacturer, outsources a number of its manufacturing orders to overseas companies such as YiFeng, an automotive die vendor. Under normal circumstances, American Tooling would submit orders to YiFeng and YiFeng would start production and bill American Tooling in stages. Upon receiving a bill, American Tooling would wire payment. At some point, a fraudster hacked the email of a YiFeng employee and sent several invoices to American Tooling, directing an American Tooling employee to wire payments to a different account. American Tooling discovered the fraud when YiFeng sent the actual invoices, but by then it had already wired \$834,000 into the fraudulent accounts.

American Tooling made a claim for the loss under the “Computer Fraud” provision of its Travelers “Wrap+” business insurance policy. Travelers denied the claim, arguing, among other things, that American Tooling did not suffer a “direct loss”; the fraudster’s conduct did not constitute “Computer Fraud”; and that the loss was not “directly caused by Computer Fraud.” The district court agreed with Travelers and granted summary judgment.

The Ruling

The Sixth Circuit reversed, holding that the policy did indeed afford coverage for American Tooling’s loss.

In its decision, the Sixth Circuit first discussed Travelers’ claim that there was no “direct loss.” Just like the court in *Medidata*, this Court held that American Tooling had suffered an immediate and direct loss. The Sixth Circuit reached the same conclusion as the Second Circuit by equating “proximate cause” with “direct cause” for purposes of Computer Fraud protection.

The Sixth Circuit also held that the fraudster’s conduct constituted “Computer Fraud”:

Travelers’ attempt to limit the definition of “Computer Fraud” to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured’s computer is not well-founded. If Travelers had wished to limit the definition of computer fraud to such criminal behavior it could have done so. Because Travelers did not do so, the third party’s fraudulent scheme in this case constitutes “Computer Fraud” per the Policy’s definition.

Finally, the Court disposed of Travelers’ other arguments, stating that American Tooling’s loss was directly caused by “Computer Fraud” and that none of the exclusions—read in favor of the insured and against the drafter—are applicable to this claim. The district court’s grant of summary judgment in favor of Travelers was reversed based upon the panel’s finding of coverage.

Key Takeaways

The Sixth Circuit's holding in *American Tooling* is significant for policyholders on many levels. First, just as the court did in *Medidata*, this court held that "proximate cause" qualifies as "direct loss" in the context of Computer Fraud insurance coverage. Since corporations cannot act outside of their employees and most wire or cyber fraud losses pass through multiple employees before money is transferred, this broad reading of "direct loss" provides significantly more coverage. Second, the case provides more clarity on the meaning and application of key provisions in Computer Fraud coverage. This guidance helps policyholders and their advisors to understand how these relatively new insurance products apply in practice. Finally, this decision further tilts the circuit split on "direct loss" in favor of policyholders.

As these recent cases show, many companies that do not traditionally think of themselves as technology-based are at risk for cyber-related losses. Through "phishing", spoofing, and social engineering, fraudsters and hackers will exploit a company's weakest point – where technology intersects with employees. As cyber risk policies mature, and cyber fraud becomes more prevalent, crime insurers are starting to exclude these types of claims. Now, more than ever, it is important to fully understand what your insurance covers and where there may be potential gaps, so you can appropriately manage your risks.

SDV's coverage attorneys have experience in both cyber risk and crime coverage. You can send us an email at coverage@sdvlaw.com or give us a call at (203) 287-2100 and you will be directed to an experienced cyber risk attorney.

* Andrew Heckler is a Summer Associate at Saxe Doernberger & Vita, P.C.