How Civil RICO Litigation Can Help Companies Recover Their Data After a Cyber Attack

By Kamal Ghali and John Floyd

As millions of Americans continue to work from home through the COVID-19 pandemic, the risk of cyber attacks, data leaks, and insider thefts will continue to skyrocket. And it may be months before corporate data breach victims learn about what may be ongoing breaches and massive thefts. As some of the biggest companies in the U.S. have learned firsthand, corporate data breach victims often find themselves scrambling to recover their data after a malicious cyberattack. Whether it's the theft of trade secrets, patient data, proprietary source codes, detailed manufacturing processes, or even embarrassing emails, companies have a limited range of options for actually getting leaked or stolen data back.

But there are a number of civil litigation tools that companies should consider using once they learn that data has been leaked or stolen. One powerful—but often overlooked—vehicle for potentially recovering stolen data is the Georgia Racketeer and Influenced Corrupt Organizations Act's robust civil remedy provision.

Consider, for example, an all too familiar set of scenarios involving malicious insiders: An employee downloads troves of data before leaving the company; a current employee remotely conducts late-night downloads of valuable company information for no obvious work-related reason; or a disgruntled insider threatens to disclose sensitive data unless his settlement demands are met. By the time the company finds out, the insider may have already transmitted the data to third parties. To make matters worse, such insiders may be storing company data in personal laptops, various storage drives, email accounts, cloud-based servers, and other places beyond the immediate reach of the company. The huge increase in the number of employees working from home only magnifies these risks.

Such thefts almost certainly violate a host of state and federal criminal statutes, including federal prohibitions on mail and wire fraud, computer fraud and abuse, and Georgia's sweeping theft by taking statute, which prohibits the unlawful taking of "anything of value," including intangible property.

In Georgia, corporate victims of such flagrant and repeated criminal conduct should consider using the Georgia RICO Act's broad civil remedy provisions to help reacquire lost or stolen data. For example, Georgia RICO bars individuals from acquiring or maintaining an interest in any personal property through a pattern of racketeering activity.

Notably, Georgia's RICO statute, like that of several states, authorizes judges to issue a broad array of "appropriate orders and judgments" to enjoin violations of the statute. Where a company has identified a specific employee in possession of stolen data, a court could direct the employee to immediately surrender all stolen data and appoint a receiver or master to review certain email and online storage accounts for the purpose of retrieving any stolen data. Depending on the facts, the court might direct the defendant to identify logins, passwords, and any other accounts capable of storing data. Assuming the company could make an appropriate evidentiary showing, it could request a civil seizure order authorizing a narrow and targeted seizure for the purpose of reacquiring stolen data.

Georgia RICO also creates the possibility of obtaining injunctive relief against third parties in possession of a company's stolen data. After all, individuals or entities that "receive" stolen property or retain it after they know (or should know) that the property was stolen may be acting in violation of Georgia's broad "theft by receiving stolen property" statute. A thoughtfully crafted injunction might direct third parties in possession of such data to destroy or return the stolen information.

While corporate victims will consider using other statutes, such as federal and state laws banning trade secret theft to get their property back, a state RICO statute may be more effective. For example, even where an attacker steals an actual trade secret (as opposed to other sensitive data), a plaintiff must still show that it took reasonable measures to maintain the secret. In many cases, companies may not be able to make that showing. On the other hand, a corporate victim's failure to securely maintain data is not a defense to a criminal theft or to a suit for injunctive relief under Georgia RICO.

Even before the COVID-19 pandemic, too many organizations were unprepared for the fallout from a malicious cyber attack. The chaos unleashed by COVID-19 has further strained the focus and attention of most organizations. And large-scale layoffs run the risk of creating a substantial cohort of disgruntled former employees with access to sensitive information. When it comes to addressing cyber threats by insiders, companies should ensure that their outside counsel have a range of plans in place to claw back stolen data, including plans for quickly initiating civil litigation where appropriate. Where companies learn about an ongoing theft in time to fight back, Georgia's RICO statute is a potential vehicle for containing the fallout from a malicious insider attack.

Kamal Ghali is a former deputy chief of the cyber and intellectual property crime section at the U.S. attorney's office in Atlanta and leads the cyber and digital litigation practice at Bondurant, Mixson & Elmore. He can be reached at ghali@bmelaw.com.

John E. Floyd is a partner at Bondurant, Mixson & Elmore and the author of "RICO State By State: A Guide to Litigation Under the State Racketeering Statutes" (American Bar Association, Section of Antitrust Law 2011 and 1998). He can be reached at floyd@bmelaw.com.

A previous version of this article appeared on Law.com on May 31, 2019.