

BUSINESS LAW TODAY

From Victim to Victor: Corporate Crime in the Internet Era

By [Mark Mermelstein](#) and [Mona S. Amer](#)

Crimes such as data breach, theft of intellectual property such as trade secrets, and the sale of counterfeit goods have reached epic proportion. Currently, the estimated annual cost of global cybercrime is \$100 billion, with over 1.5 million victims per day, and more than 232.4 million identities exposed per year. This year, 59 percent of ex-employees admitted to stealing company data when leaving previous jobs. In 2011, the anti-piracy consortium Business Action to Stop Counterfeiting Piracy of the International Chamber of Commerce estimated that the yearly cost of counterfeiting and piracy is \$775 billion, and is expected to reach \$1.7 trillion by 2015.

Just this year, more than a dozen American and international corporations, including Nasdaq, 7-Eleven Inc., and J.C. Penney Corp. suffered data breach incidents resulting in the exfiltration of more than 160 million credit and debit card numbers, causing those companies hundreds of millions of dollars in losses. Last month, it was reported that three Eli Lilly employees walked off with \$55 million worth of their employer's trade secrets that they then sent to a competing Chinese drug company. In June of this year, trademark holders including Nike, Tiffany & Co., and the four American professional sports leagues all had their trademarks violated by counterfeiters selling knock-offs over the Internet.

Each one of the companies mentioned above was the victim of a crime. Individuals typically don't like to be perceived as victims. The same – perhaps to an even greater degree – holds true for corporations. Being a victim is unlikely to enhance a company's reputation. Even worse, if the company's brand (such as a bank's), is built around keeping client assets or information confidential, admitting that one has been the victim of data breach can significantly undermine the company's mission. However, embracing their statuses as victims of crimes is what each of the above-mentioned companies did. Why would they do this? Unless a corporation appreciates its status as a corporate crime victim, it may not be aware of all of its available options for recovery for the harm the perpetrators have caused. Consider some of the advantages of embracing being a corporate crime victim, or "CCV." CCVs, like all other crime victims, have statutory rights. They get the benefit of having the government work for them to investigate, prosecute, restrain the liberty of, and collect money from the perpetrators. Where the perpetrator is an employee, being a CCV may allow the corporation to insulate itself from liability for a perpetrator's acts. Oftentimes, CCVs can collect insurance proceeds from their fidelity/crime policies. While wrapping oneself in the CCV flag may not be the solution to

all of the above misconduct, it is one tool in the toolbox that should be considered alongside other more commonly used tools to redress injury, such as civil litigation.

Companies that have positioned themselves as CCVs have begun to see and take advantage of its benefits. Consider the case of former Goldman Sachs director Rajat Gupta. In 2012, Gupta was prosecuted for insider trading and convicted of conspiracy and securities fraud. As a result of Gupta's conduct, Goldman Sachs spent millions of dollars fending off actual and potential legal attacks related to its responsibility for Gupta's conduct and otherwise facilitating Gupta's prosecution. Goldman, long considered a Wall Street maverick, embraced the concept that it was a CCV, a victim of Gupta's insider trading.

Although insider trading has long been considered a victimless crime, Goldman exercised its rights as a victim of Gupta's crime to appear at Gupta's criminal sentencing and demand restitution for the injury it suffered at Gupta's hands – the expenditure of significant attorney's fees. In February of this year, Gupta's sentencing judge ordered Gupta to pay Goldman Sachs \$6.2 million in restitution to reimburse Goldman Sachs for the legal fees it incurred during its internal investigation of Gupta's conduct, as well as during its cooperation with the government's investigation

and prosecution of Gupta.

Pursuant to the Mandatory Victims Restitution Act (MVRA), a “victim” is defined as “a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered. . . .” 18 USC § 3663A. Goldman was able to position itself as a CCV, fended off any suggestion that it shared liability for Gupta’s misconduct, and received a \$6.2 million restitution order. For companies that find themselves involved in misconduct such as that described above, it may well be worth considering some of the advantages of being a CCV as compared to merely being a tort victim suing in civil court.

The Government Investigates the Crime

Once an alleged crime has been referred to the government, government agencies, not the victim, investigate the wrongdoing. Indeed, the government has powers and resources above and beyond those available to private sector investigators or attorneys. These include the ability to obtain search and seizure warrants, obtain grand jury and administrative subpoenas, and utilize wiretaps and other forms of electronic surveillance. The government’s ability to threaten someone’s liberty is a great way to get witnesses to talk. The government also partners with law enforcement in other countries to gain the investigatory benefits that foreign sovereign law enforcement offer. For example, in the counterfeiting case described above, U.S. Immigration and Customs Enforcement’s Homeland Security officers conducted a joint investigation with European law enforcement agencies, since the counterfeiters were operating websites both in the United States and in Europe. This joint investigation culminated in the government seizing 328 websites that the counterfeiters were using to sell the counterfeit merchandise. While civil litigants do investigate and obtain subpoenas, their ability to go undercover, typically necessary in any cyber-investigation, is constrained by attorney ethical rules. For a CCV, having this investigation done by the government on the taxpayer’s dime, as opposed to by the company itself, can save

the company significant money and likely obtain results superior to what a corporate citizen or civil litigant could achieve.

The Government Locates the Criminal Wrongdoers

The government also has tools and resources to locate and arrest the responsible parties. While U.S. residents are responsible for the majority of hacker attacks on U.S. businesses, a significant number originate in eastern Europe, Germany, China, and the United Kingdom. The United States government, as part of its crime investigation, has the ability to track suspects internationally either on its own or in conjunction with local law enforcement. The government can and does routinely obtain INTERPOL warrants for the arrest of foreign nationals and extradite perpetrators from countries with which it has extradition treaties. In the hacking case referenced above, one of the foreign defendants was arrested while in the United States sightseeing and another was arrested in the Netherlands and is currently awaiting extradition.

The Government Collects from Wrongdoers

One of the government’s most powerful weapons is its asset forfeiture power. The government has the ability to seize and forfeit property of those suspected of criminal activity. This property can then be liquidated and used to provide restitution to corporate victims. For example, in the counterfeiting case described above, not only did the government seize the offending websites, it also seized more than \$150,000 in proceeds that the counterfeiters had received through the websites’ PayPal accounts. Those seized funds will be forfeited to the government, and then used in part to provide restitution to the various companies victimized by the crimes. While private attorneys do have some limited ability to seize assets via civil litigation, the government will typically have the element of surprise which is significant when trying to seize portable assets such as currency. The government can also use the threat of a lengthy incarceration to incentivize crimi-

nal defendants into revealing the location or and/or repatriating further funds for restitution.

Companies Can Recover Under Their Fidelity/Crime Insurance

Many corporations invest in fidelity insurance that provides coverage for crimes such as employee theft and computer fraud. Collecting under a policy like this can be a significant source of recompense for injury to the victim corporation. However, oftentimes as a prerequisite to recovery from an insurance company, many policies require that the corporation report that crime to law enforcement.

Companies Attain Rights to Restitution and Cost Recovery

The Crime Victim’s Rights Act (CVRA) affords crime victims various rights, including “[t]he right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused,” “[t]he right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding,” “[t]he reasonable right to confer with the attorney for the Government in the case,” and “[t]he right to full and timely restitution as provided in law.” 18 U.S.C. s. 3771(a)(3), (4), (6). The rights afforded under the CVRA are available to corporate entities. *United States v. Dreier*, 2013 U.S. Dist. LEXIS 92863 (S.D.N.Y. July 2, 2013).

Under the Mandatory Victims Restitution Act, any assets that are forfeited to the government or are turned over to the government can be used to compensate victims of certain crimes. This includes funds that are seized from the criminal defendants, like the ill-gotten gains that were seized from the counterfeiters, or assets that were purchased with illegally obtained funds.

Not only can a company receive restitution to compensate for the crime, it may also be able to recover amounts it expended on investigating the wrongdoing. Case law has been developing around the MVRA that allows companies to receive restitution from

wrongdoers. In addition to the Goldman Sachs restitution award described above, former J.P. Morgan managing director Joseph Skowron III was ordered to reimburse J.P. Morgan for the fees it incurred investigating Skowron, who was subsequently charged with securities fraud and obstruction of justice, as well as the fees the firm incurred cooperating with the SEC during its investigation. In July of this year, the Second Circuit Court of Appeals affirmed the restitution order. The advantages of being a CCV are clear: although fees spent on internal investigations will be incurred in virtually every case of insider or employee criminality, those fees are not recoverable in civil litigation.

Companies Gain an Advantage in the Public Relations Battle

In data breach cases, attorneys general often bring civil lawsuits under their consumer protection auspices, as do consumers whose private data has been exposed. When a civil lawsuit is commenced against a corporation that understands its status as a CCV and has gotten the government involved to pursue the perpetrators, the corporation can obtain an advocacy advantage by positioning itself first and foremost as the victim of a crime, and forcing the role of principal tortfeasor onto the person who committed the theft or cybercrime. By deflecting blame onto the more significant wrongdoer, the company may make itself appear more sympathetic and make the litigation more challenging to pursue. In both litigation and public relations, wearing the white hat can yield intangible benefits.

Conclusion

To be sure, there are potential downsides to admitting one's status as a CCV and inviting the government into a corporation's affairs. While the company controls any civil litigation it initiates, the company cannot control the government's criminal investigation. Similarly, if the government moves forward to prosecute a case, facts embarrassing to the CCV will probably need to be turned over to the government and thus the confidentiality of that information

can no longer be assured. As a result, the status of a CCV and referring the matter to the government is not a panacea. For CCVs who have suffered from data breaches, counterfeiting, or employee theft, there is typically concurrent jurisdiction to proceed by way of civil litigation, criminal referral, or both. Corporations that are reticent to embrace the status of a CCV may thereby be foregoing the best avenue to redress their injuries. Adopting CCV status is an option worth considering, particularly in situations where the facts of the case will become public anyway (because, for example, a data breach statute requires consumer notification).

[Mark Mermelstein and Mona S. Amer](#) are partner and of counsel, respectively, in Orrick, Herrington, Sutcliffe LLP's White Collar Crime and Corporate Investigations practice. In addition to criminal defense, they spend time representing corporate crime victims.