JOURNAL OF INTERNET LAW
VOLUME 16
NUMBER 12
JUNE 2013
EDITED BY DLA PIPER

Strategic Remedies for Cybercrime Victims

By Mark Mermelstein, Mary Kelly Persyn and Harry J. Moren

An industrial equipment manufacturer calls. Somehow, an intruder has hacked into its Website and used that portal of entry to locate and steal proprietary trade secrets. Now a Chinese competitor is using the stolen information to manufacture and sell counterfeit versions of the client's products over the Internet.

A major Internet Service Provider reaches out to your firm, hoping you can help stem the tide of spam that is drowning its subscribers and threatening its business. Some of the subscribers are themselves falling victim to phishing scams and are being tricked into parting with either money or confidential personal information. The company representative explains that battling spam is very much like trying to exterminate cockroaches. The company can go after individual addresses, but can't figure out how to shut down larger spam-generating operations.

What should an attorney tell these cybercrime victims? The traditional solution for these tort victims is initiating a civil lawsuit against the perpetrator in order to obtain a money judgment, and then turning that money judgment into cash to compensate the victim for its losses. But this approach may not necessarily make sense in the Internet era, which offers a number of challenges for the civil litigant. Consider the following:

- The Internet offers a degree of anonymity to the perpetrator. Finding the perpetrator is often a prerequisite to getting him or her to pay;

Continued on page 21

Mr. Mermelstein, Ms. Persyn, *and* ***Mr. Moren*** *are employed at Orrick, Herrington & Sutcliffe in its Litigation Department. Mr. Mermelstein is a partner in Orrick's White Collar & Corporate Investigations practice and represents both white collar criminal defendants and corporate crime victims. Ms. Persyn is a managing associate in Orrick's White Collar & Corporate Investigations and Appellate practices; she represents white collar criminal defendants and handles appellate matters for a range of clients. Mr. Moren is an associate in the firm's General Litigation practice.*

Wolters Kluwer
Law & Business

Strategic Remedies for Cybercrime Victims from page 1

- By reaching through the Internet to commit a crime like theft, the perpetrator—as well as the assets that one could liquidate to satisfy a judgment—are often on a different continent than the victim;
- For a counterfeiter, using the Internet and the virtually infinite number of Web addresses that it makes available as distribution channels means that even if one distribution channel is shut down, another may pop up.

Circumstances like those described above therefore present unique obstacles to remedying the harm caused. It may be extremely challenging if not impossible to locate the perpetrator(s) in either of these examples. Even assuming that a litigant succeeds in locating and suing a perpetrator, the money judgment awarded as a result is only the first step in asset recovery. Payment is not forthcoming simply because a judgment has been rendered. Turning that judgment into money may be a long road requiring enforcement of the judgment, and locating and liquidating the perpetrator's assets in a foreign country that may not be terribly hospitable to the litigant's efforts. Similarly, it's not clear that any injunctive relief obtained would actually be effective in causing the offending conduct to stop. A likely outcome at the end of traditional civil litigation is a litigant with little more than a piece of paper to show for its efforts. As such, even in situations where the perpetrator's liability may be clear, a traditional civil lawsuit may not be effective, let alone cost-effective.

Significantly, there are other tools in the toolbox of the Internet-era lawyer. These new-era tools include a criminal referral, an International Trade Commission complaint, and a modern civil litigation approach. The criminal referral—referring the matter to a criminal prosecutor to investigate and initiate criminal proceedings against the perpetrator—takes advantage of the fact that the government has institutional advantages over civil litigants when it comes to investigation and asset collection. Filing a complaint before the International Trade Commission, which has the power to enjoin a company from importing a product derived from an unlawful business practice, may make more sense than suing a foreign company in civil court. Finally, if a spammer's goal is to send as much spam as possible, the solution may be to dismantle the spammer's operation computer by computer, rather than to obtain a money judgment. Modern civil litigation may be just the vehicle to achieve that end.

To be sure, before taking any of the tools out of the toolbox, an effective practitioner must understand the facts and the victim's goals. There simply is no substitute for investigation on the front end of a case. A practitioner should learn as much as he or she can about the victim, the perpetrator, the breadth and depth of the perpetrator's conduct vis-à-vis the victim, and whether this perpetrator has done this type of thing before. Because of the especially technical nature of cybercrime investigation, it may make sense to bring in forensic consultants or private investigators. The key, though, is that the entire investigation should be covered by the attorney-client privilege and therefore protected from forced disclosure. An attorney can lead the investigation and engage private investigators, forensic investigators, and others to assist. Acting as the attorney's agents, these individuals' findings will typically be protected by the attorney–client privilege unless and until the client chooses to waive that protection. The protection afforded by the privilege is critically important because it's never clear what one will find at the start of an internal investigation. Especially when a client may have an area of vulnerability, it's best to have control over the information in the event that what the investigation turns up—for example, involvement in the criminal enterprise by a high-level employee of the victim company—is something that the client wants to reveal only on its own terms, or does not want to reveal at all. The goal is to understand the level of victimization and any potential collateral consequences that could result from the use of any of these tools before employing any of them.

In addition to understanding the facts, the wise practitioner should understand the client's goals. Is the client looking for the offending conduct to stop? Is the client looking to obtain compensation for losses? Is the client, such as a bank, concerned about the adverse public relations it may suffer if it becomes known that it wasn't able to effectively safeguard its customer information?

It is similarly worth investigating any potential sources of money that can help defray the victim's costs. Does the victim have a cyber-insurance or other insurance policy that provides coverage? Answers to these questions will influence the choice of tool for the job.

Additionally, if the decision is ultimately to make a criminal referral, an internal investigation has the further advantage of making it more likely that the government will accept the referral and prosecute the case. While the government has greater powers of investigation, enforcement, detention, and asset seizure than private individuals, by handing the government a well-researched and neatly tied-up investigation, the attorney increases the chances that prosecution will be brought and hastens the government's ability to proceed.

CRIMINAL REFERRAL

While civil suits can be effective in cases of cybercrime, a referral to law enforcement authorities could be a client's best route to asset recovery. The investigatory and prosecutorial powers of the government are immeasurably more powerful than anything available to a private litigant in a civil litigation. The government has wiretap powers; given sufficient cause, it can investigate in secret; it can conduct raids and disable criminal operations; it can charge individuals with a crime; and it has tremendous asset seizure authority. However, there are risks to a referral that must be weighed in the balance.

INVESTIGATORY ADVANTAGES

Consider the investigatory advantages that the government has over a private litigant. Investigation can be divided into formal methods, such as invoking the formal processes of a court to obtain documents via a subpoena or testimony via a deposition, and informal methods, such as requesting that people speak or hand over documents. Where the hope is that the target of the inquiry will by informal methods or voluntarily disclose information, it is clear that the gun and badge of law enforcement are a lot more intimidating than the bar card of an attorney. In the presence of law enforcement, people hand over information they simply would not when confronted by an attorney.

Given that one of the biggest challenges in responding to cybercrime is identifying the perpetrator, what about assuming a false identity and participating in Internet chat rooms and other fora with the goal of locating and ultimately identifying the perpetrator? The government is well within its rights to do this. Government agents can pose as an underage girl and participate in chat rooms to entice adult men; certainly government agents can go undercover and pose as hackers trying to gain the confidence of fellow hackers.

For civil lawyers, however, the answer is less clear. A number of state bar opinions have stated that deceptive practices such as these may violate an attorney's ethical obligations. Can an attorney misrepresent her identity and pose as a "friend" to gain access to someone's private Facebook page? Presumably this ruse is necessary because if the attorney presented her true identity, she would be denied access. In that light, Rule 4.1 of the American Bar Association's Model Rules of Professional Conduct advises that "[i]n the course of representing a client, a lawyer shall not knowingly: make a false statement of material fact or law to a third person."[1] In California, which has not adopted the Model Rules, it is the duty of a California lawyer "to employ for the purpose of maintaining the causes confided to him those means only as are consistent with the truth, and never seek to mislead a judge…."[2] The California rule does not clarify whether the prohibition on making false statements applies in general or only with respect to in-court representations. At this point, at least San Diego and Philadelphia Bar Association opinions suggest that these types of deceptive attorney investigation are prohibited.[3] It is unlikely that an attorney could hire a private investigator to do that which the attorney cannot do directly.

When it comes to formal investigatory techniques, at least in theory, the government and private litigants are on an even playing field: they can all obtain the power to serve subpoenas. Criminal prosecutors have subpoena power via a grand jury; many agencies can also obtain an administrative subpoena. In contrast, a private litigant must obtain subpoena power by initiating a lawsuit. Even if the investigation is at a preliminary stage, a private litigant who has not yet identified the perpetrator can initiate a John Doe

lawsuit alleging that certain as-of-yet unidentified perpetrators have committed a tort. Even though the legal effect of the subpoena—an enforceable order to comply—is the same whether it is a private litigant or governmental subpoena, response to a governmental subpoena tends to be more fulsome. This is because noncompliance with a government subpoena may result in criminal obstruction of justice, whereas noncompliance with a civil subpoena typically results in motion practice before a trial court and perhaps a small monetary sanction.

In cybercrime investigations, the key question is whether the victim will be able to look past an IP address or domain name associated with the criminal activity and discover the identity of the perpetrator. After identifying the Internet Service Provider ("ISP") or domain registry associated with the offending IP address or domain name, the next step is to reach out to that third party to find out the name of the subscriber associated with it. Subscriber information is generally available to both the government and private litigants via subpoena. If information beyond the subscriber's identity is at issue, such as the content of emails, the contrast is starker still. In the private-litigant realm, the Electronic Communications Privacy Act ("ECPA") prohibits a litigant from obtaining email content from an ISP; this means that this information is available only via voluntary disclosure or consent.[4] In the government arena, the ECPA regulates how the government can obtain stored account information from the ISP. Some information can be voluntarily disclosed. A criminal prosecutor can serve a subpoena on the ISP without notice to the subscriber to obtain the name, address, telephone connection records, records of session time, duration, and means of payment for service. If the criminal prosecutor serves a subpoena on the ISP with notice to the subscriber, in addition to the previous information, the government can obtain the contents of email in storage for more than 180 days.[5]

If the information available by subpoena is insufficient for the government's purposes, it can obtain an order under ECPA Section 2703 ("2703 Order"). With a 2703 Order, the government can, without notice to the subscriber, obtain account logs and transactional records, in addition to all information listed above.[6] If the government obtains a 2703 Order and provides notice, it can obtain all of the information listed above, plus all opened email regardless of its age. To get a Section 2703 order, the government must show "specific and articulable facts showing that there are reasonable grounds to believe" that the contents of the information sought are "material to an ongoing criminal investigation." Thus, distinct from a subpoena, the government needs to actually articulate the facts. Finally, the government can get an order constraining the ISP from disclosing to the subscriber the fact that the ISP has provided information to law enforcement. The justification is investigation confidentiality.

Both with respect to ISPs and beyond, the government uniquely has the ability to obtain and execute a search warrant. With a wiretap warrant, the government can monitor a hacker as she breaks into a victim's computer system and wiretap a suspect's phone to learn whom the suspect has called. Private litigants generally do not have this power; however, a victim may have implicit consent to monitor subscriber use on its computer systems via a user agreement or banner.

The government can obtain "cell-site" location information from a suspect's cell phone to determine a suspect's approximate location at the time of a call.[7] In the case of computer searches, though, the government may be at some disadvantage, being bound by the Fourth Amendment for such searches while a private litigant is not.

When dealing with evidence located outside the United States, the government is uniquely situated to team up with foreign law enforcement to obtain information, either informally or through a mutual assistance legal treaty.

COLLECTION ADVANTAGES

Moving beyond investigation, the government's collection powers, i.e., the ability to obtain compensation for crime victims, are also far superior to those of private litigants. While private litigants must, with limited exceptions, rely on first winning a lawsuit and then winning the long battle of attrition to enforce a money judgment that follows, the government has many means at its disposal to gain nearly immediate relief for a victim. For example, with a forfeiture warrant, the government can seize assets within its jurisdiction that are either the instrumentalities or

fruits of the perpetrator's crime. These assets can be converted into funds to compensate a crime victim.

Most significantly, the government wields the ultimate hammer: criminal prosecution. Loss of liberty creates formidable leverage. After a successful criminal referral, the victim is able to appear at the criminal defendant's sentencing, can seek restitution, and is allowed to speak about his victimization. In many states, an attorney cannot use the threat of criminal prosecution to force an individual to part with assets,[8] but, mindful of avoiding this ethical prohibition, bargaining-chip possibilities exist.

After conviction, one could approach the defendant and conduct a negotiation in advance of the sentencing hearing. Since judges take restitution and remorse into account when deciding to what extent a deprivation of liberty is appropriate, an opportunistic victim may seek that moment to make a restitution demand. When deprivation of liberty is in the offing, criminal defendants tend to be willing to part with their money much more readily than they would in the face of a mere civil judgment. Indeed, this method of asset recovery has been codified in California, where "civil compromise" allows a court to dismiss a misdemeanor if restitution has been made to the victim.[9]

The effectiveness of two of the government's chief collection mechanisms—asset forfeiture and threat of prison time—is illustrated by the following case handled by one of the authors of this article. His client paid a gallery owner $2 million for a painting titled "La Femme au Chapeau Bleu," ostensibly a 1902 pastel by Pablo Picasso. Later, the client learned it was a fake and that the client had been defrauded by the gallery. Owing to a series of prior bankruptcy filings and significant encumbrances on the only real property owned by the gallery owner, collection on a civil judgment did not seem promising. Instead, a criminal referral was made. The criminal authorities tracked down the person who had created the fake (for less than $10,000), arrested the gallery owner, and filed charges. Because the government had evidence that the ill-gotten gains had been used to purchase a DeKooning painting, the government was able to seize it under its asset forfeiture powers. Recognizing that the gallery owner was facing prison time for these misdeeds, the gallery owner's criminal defense attorney called with a proposal: the gallery owner would agree not to contest the DeKooning being turned over to the client, discharge some of the senior liens on the property, and give the client a lien. In exchange, the client would inform the court of the nature and extent of the defendant's cooperation with regard to restitution. All told, the client recovered more than $2 million, more than the actual amount of the fraud. No doubt, the government's collection powers—asset forfeiture and threat of liberty deprivation—inured directly to this crime victim's benefit.[10]

CRIMINAL REFERRAL FOR CYBERCRIME VICTIMS

But the story of the fake Picasso painting involves an identified perpetrator with a brick-and-mortar business and readily identifiable assets. Sales of counterfeit goods over the Internet present classic cybercrime characteristics that foil traditional approaches. Any retailer of licensed goods is at risk.

With respect to the industrial equipment manufacturer discussed earlier whose trade secrets have been stolen and whose goods are being counterfeited, civil options are few. Because sellers of counterfeit goods over the Internet can hide behind its anonymity, it could be impossible to remonstrate with the Chinese perpetrator, let alone negotiate. A civil suit, which would be very difficult to conduct, could result in an injunction prohibiting a particular Web site from selling the product, and perhaps some product can be seized and destroyed. However, there are significant challenges to identifying the actual people who run the Web site. And even if a judgment results, enforcing it in China would be nearly impossible.

Criminal referral is an interesting alternative here for several reasons. One of the most valuable tools in law enforcement's arsenal in this context is seizure of the domain names used by counterfeiters. In November 2012, a "Cyber Monday" crackdown by United States Immigration and Customs Enforcement, in cooperation with law enforcement from several other countries, seized 132 domain names used to traffic in counterfeit goods.[11] The crackdown focused on trademarked goods. The sites were first identified by means of undercover purchases; the Justice Department then obtained seizure orders for the domain names. After the owners failed to appear and claim ownership, the government could

lawfully seize and destroy the domain names. All told, the Justice Department's Task Force on Intellectual Property, chaired by Deputy Attorney General James Cole, which has dedicated to it fifteen Assistant United States Attorneys and twenty FBI agents, has to date seized nearly 1,000 domain names.

In addition to seizing domain names, the government has had success seizing money for the benefit of counterfeiting crime victims. In an operation conducted by the IP Task Force in 2012, a Chinese counterfeiter's PayPal account was seized, along with funds paid to PayPal by customers but not yet distributed to the counterfeiter.[12] Further, the government can seize assets that have been deposited in a U.S. branch of the counterfeiter's foreign bank—in this case, the Bank of China. Even if the assets have already been transferred offshore, the government can still seize other Bank of China funds within the United States on the theory that the bank can then go after the counterfeiter's account in China for reimbursement. Using these techniques, the government recovered nearly $1 million for the victims of this particular counterfeit scheme.[13]

While it can be challenging to find a law enforcement agency to take a criminal referral, the IP Task Force has the technical expertise, funding, and manpower to take on cases involving counterfeiting and other IP fraud and crime.

Another aspect of the criminal referral bears mention—the ability of the crime victim not just to recover the direct loss resulting from the criminal conduct, but also attorneys' fees spent investigating the perpetrator and filing a restitution claim. On February 25, 2013, former Goldman Sachs director Rajat K. Gupta was ordered to reimburse Goldman Sachs $6.2 million for legal fees Goldman Sachs incurred in its internal investigation into Gupta's illegal insider trading activities.[14] Some states also have laws that award attorneys' fees to crime victims generally.[15] By contrast, in the civil context, these categories of fees are not recoverable; if trade secrets are stolen, a successful tort lawsuit for theft of trade secrets does not normally yield an award of attorneys' fees.

Since any experienced prosecutor will want to understand potential areas where the criminal defendant may cross-examine the victim, the prosecutor will want to explore the victim's conduct before hearing the cross-examination results at trial. Any attorney considering a criminal referral needs to have a very frank and probing conversation with a client to ensure that if the referral is made, the client does not have any "areas of sensitivity" that would then expose the client to potential prosecution by the very same prosecutor invited into the case. Attorney and client should also remember that once the referral is made, it cannot be unmade, and the government will take the case over entirely; control over the direction and ultimate end of the case will be lost.

In sum, referral to a government agency has clear advantages in terms of investigatory and prosecutorial power and ability to recover assets. However, if the victim would be vulnerable if investigated, referral may not be the answer.

ACTIONS BEFORE THE INTERNATIONAL TRADE COMMISSION

Consider again the hypothetical introduced earlier involving the industrial equipment manufacturer who is the victim of a theft of trade secrets, the fruits of which are being sold into the U.S. market.

Where the perpetrator of the crime takes advantage of the ill-gotten gain by importing goods into the United States, filing a complaint with the United States International Trade Commission ("ITC") is an another option worth considering. Even if a perpetrator is hard to find, the ITC has jurisdiction over relevant assets in the United States; the proceedings are much quicker than the typical federal district court litigation; and the administrative law judges who conduct the proceedings are technologically sophisticated. Though it cannot order money damages, the ITC can issue exclusion orders and cease-and-desist orders. And its proceedings can then be used in federal court to pursue money damages.

The ITC, an independent, quasi-judicial federal agency, administers U.S. trade remedy laws and has statutory power to grant relief for many types of anti-competitive harm, including import practices involving the infringement of a U.S. patent, copyright, or trademark; misappropriation of trade secrets; and false advertising.[16] The types of relief available are exclusion orders, which exclude an infringing good from entry into the United States, and cease-and-desist orders, which command an entity to cease and desist

specified conduct or face a statutory civil penalty.[17] Expedited preliminary relief—a temporary exclusion order or a temporary cease-and-desist order—is also available.[18]

Procedurally, a victim's complaint triggers initiation of an adversarial proceeding before an administrative law judge through which the victim can obtain an order prohibiting the importation of the infringing goods. Instigating an ITC proceeding can be advantageous when the perpetrators are anonymous or difficult to reach because the agency has *in rem* jurisdiction over goods imported in the United States.[19] Demonstrating personal jurisdiction over the perpetrators is not necessary. Of the advantages an ITC proceeding affords, a significant one is discovery.[20] Because it is a federal agency, the ITC has national third-party subpoena power that exceeds the jurisdiction of federal district courts, which may issue third-party subpoenas only within particular geographical areas. In a federal district court litigation, to serve a subpoena nationally but outside the court's particular geographic region, one need initiate another proceeding in a federal district court in the geographic area where the information lies. Given a subpoena that calls for a wide array of documents, a federal district court that is otherwise unfamiliar with the underlying federal civil litigation may grant the subpoenaed party leeway in objecting to the burden of production; the ITC, however, tends to take a broad view as to what needs to be produced. Similarly, extraterritorial discovery in ITC proceedings tends to be more fruitful than in a federal civil litigation. If the perpetrator is located in China, for example, propounding a civil subpoena issued as part of a civil litigation will not yield results because it will not be enforced in China. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters governs extraterritorial discovery in a civil lawsuit,[21] but the process is cumbersome and generally ineffective. When the extraterritorial subpoenaed party bears some relationship to one of the parties before the ITC—for example, a subsidiary—the ITC tends to take an expansive view of the nature of the connection between the subpoenaed party and the respondent, and errs on the side of increased discovery. As a result, the ITC will often require production of evidence in the hands of witnesses or evidence affiliated with but not directly connected to a party before the ITC; a federal district court would relegate the party seeking the information to pursuing its remedies under the Hague Convention.

As mentioned above, a victim cannot recover lost assets directly through an ITC proceeding. However, similar to the threat of imprisonment in a criminal referral, an ITC proceeding carries the threat of excluding the perpetrator's products from the U.S. market. For some foreign businesses, this is a serious threat which can be used as leverage for negotiating an advantageous financial settlement.

In front of the ITC, the complainant victim of trade secret misappropriation must show substantial injury to a domestic industry.[22] The victim will need to show that there is a domestic industry for the product. An industry qualifies if the victim can show that it is making significant investment in plant and equipment; significant employment of labor or capital; or substantial investment in its exploitation, including engineering, research and development, or licensing. A recent expansion of the law now covers victims that license innovative technology, but do not manufacture.[23] Furthermore, the industry must directly relate to the stolen articles that the victim claims are protected by the relevant patent, copyright, trademark, mask work, or design. Assuming the domestic industry requirement can be met, the ITC can be a valuable forum of redress for certain cybercrime victims.

THE ITC COMPLAINT FOR THEFT OF TRADE SECRET CYBERCRIME VICTIMS

In today's business environment, trade secrets are often stored electronically on company intranet sites, which are separated from the company's internet site. But hackers have many ways to access "secure" intranets from the Internet. They can penetrate corporate firewalls and circumvent or shut down antivirus defenses. They can sneak through poorly protected wireless networks or mobile devices. They can lure employees to follow a malicious Internet link or open a doctored e-mail attachment. They can run "dictionary" attacks to overcome weak passwords. Once a hacker obtains access to a company's intranet, the perpetrator has the same access

to electronically-stored sensitive information as an employee or an IT systems administrator.

For crime victims like the industrial espionage crime victim in the hypothetical, a traditional civil lawsuit may not make sense. Consider the case of cybercrime victim Super Vision International, an Orlando-based industrial lighting manufacturer.[24] In 2000, an intruder breached Super Vision's public Web site and probed deep enough into its network to snatch secrets regarding the company's patented fiber-optic technology. Chinese competitors, who may have commissioned the cyber attack, obtained the information and used it to manufacture and sell counterfeit products.

Super Vision filed suit in Florida state court against the competitors, who allegedly destroyed documents to prevent their use as evidence. Super Vision then hired private investigators, who obtained evidence from the competitors in Shanghai and Hong Kong by posing as rich sheiks. In court, Super Vision prevailed, with the jury awarding over $40 million. Out of court, however, Super Vision won nothing. The defendants had transferred their assets out of the United States and Super Vision has yet to collect its judgment.

The ITC has recently become a more popular forum for trade secret misappropriation matters. In the past few years, it has instituted five such proceedings: all based on misconduct in or near China.[25] The surge in popularity is due in part to the 2011 decision by the Court of Appeals for the Federal Court in *TianRui v. ITC*.[26] The court affirmed an ITC decision that the importation of railway wheels into the United States from China violated Section 337 where the Chinese manufacturer of the wheels misappropriated a manufacturing process protected under U.S. trade secret law.[27] The court found that the domestic industry requirement was met under the higher standard for misappropriation complaints, despite the fact that the trade secret holder was not currently utilizing the misappropriated process, because the imported wheels could potentially compete with wheels manufactured domestically by the holder.[28] Importantly, the court found that Section 337 reached misappropriation conduct that occurred abroad; in contrast, misappropriation claims before state and federal courts generally require that the misappropriation conduct occurred within the United States.[29]

If Super Vision had taken its case to the ITC instead of or in addition to civil court, it could have protected its domestic market with an ITC exclusion order against the competitor's products. Compared to a worthless money judgment, an ITC exclusion order may have actually disrupted the Chinese competitor's ability to profit from the ill-gotten technology.

Another problem counterfeiting victims encounter in civil litigation is establishing personal jurisdiction over the foreign perpetrator. Consider the case of CSB, a New York company that owned the trademark rights to a knife holder in the shape of a human figure.[30] Urban Trend, a Hong Kong corporation, marketed a copycat knife holder in the United States via its Web site and at a Chicago trade show.[31] A federal district court in Illinois dismissed CSB's case against the Hong Kong manufacturer because the court did not have personal jurisdiction over the manufacturer.[32] The court held that Urban Trend's mere presence at the trade show, without a specific showing of marketing or sales to Illinois residents, did not give rise to personal jurisdiction.[33] The lack of personal jurisdiction over Urban Trend would have been irrelevant if CSB had filed a complaint against Urban Trend in the ITC. With a Section 337 complaint before the ITC, CSB could have obtained orders preventing Urban Trend from importing and selling the infringing knife holder over its Web site in the United States. Furthermore, CSB would have had the assistance of governmental agencies in enforcing the orders: the U.S. Customs Service with respect to importation and the ITC with respect to sales.

In fact, the ITC has recently granted exclusion orders in response to counterfeit goods sold over the Internet. In 2006, Zippo Manufacturing Company filed a complaint with the ITC to protect itself from the importation and sale of counterfeit lighters in violation of its registered trademark.[34] In 2010, Louis Vuitton filed a similar complaint with the ITC concerning the importation and sale of counterfeit handbags, luggage, and other products in violation of its registered trademarks.[35] Each company found that counterfeit versions of their products were sold in the United States by both physical and Internet retailers, including auction Web sites such as *eBay.com*. They presented evidence of foreign manufacture (in China) of the counterfeit goods. In each case, the ITC issued a general exclusion order prohibiting importation of goods infringing the registered trademarks as well

as removing already imported infringing goods from warehouses.

As relief, the general exclusion orders were more valuable to Zippo and Louis Vuitton, and more easily obtainable, then a district court remedy. The ITC noted that the manufacturers and sellers of the counterfeit goods were easily formed and dissolved; any remedy restricted to a particular entity would be practically worthless. Similarly, the anonymity of Internet retailers means that a civil suit would be difficult to litigate and any resulting judgment would be difficult to enforce.

Finally, the speed of the proceedings gave the trademark holders timely relief. The Zippo investigation began in June 2006, the administrative law judge issued an initial determination in February 2007, and the commission issued the exclusion order in July 2007. The Louis Vuitton investigation began in January 2011, the administrative law judge issued an initial determination in September 2011 and then, after remand by the commission, a revised initial determination in March 2012. The commission issued the exclusion order in May 2012.

THE MODERN CIVIL LAWSUIT

While the traditional civil lawsuit has its challenges in the Internet age, there are nonetheless certain aspects of the civil lawsuit that remain effective. Where the perpetrators of cybercrime are unknown and unidentifiable, a civil lawsuit can be initiated naming John Does as defendants in order to gain subpoena power and use discovery tools to identify the John Doe perpetrators. A civil lawsuit can also yield an injunction that transfers the ownership of, or power over, infrastructure to the plaintiff victim. Where money damages are less interesting than disabling a powerful (even overwhelming) drag on a business, the modern civil lawsuit, replete with technological sophistication and even the element of surprise, can strike back against a seemingly nebulous perpetrator.

BOTNETS

One key method by which perpetrators commit cybercrime is by setting up a "botnet." A "botnet" is a collection of individual computers each running software that allows communication among the computers and enables the computers to take direction from "command and control" computers. The individual computers in the botnet often belong to users who have unknowingly downloaded or been infected by malicious software (known as malware) that conscripts the computer to become part of the botnet. Some of the botnet computers—the "command and control" computers—are wholly within the control of the botnet creator, the cybercrime perpetrator.

A botnet can be used to carry out a variety of cyber-misdeeds such as anonymously sending out bulk emails without the knowledge of the user who owns the compromised computer. These bulk emails can lure unsuspecting users to click on a link and thereby cause the delivery of malicious software that infects the unsuspecting user's computer, thereby conscripting it to become part of the botnet. That same malicious code can disable a company's firewall and allow a perpetrator to reach in through the Internet and steal that corporate crime victim's trade secrets. The bulk email can also invite the unsuspecting user to part with personal information and therefore facilitate identity theft or fraud. Finally, a botnet computer can be used to "proxy" or relay Internet communications originating from other computers.

USING MODERN LITIGATION TECHNIQUES TO FIGHT A BOTNET

Because most computers connected to the Internet run Microsoft Windows, Microsoft has taken a special interest in disabling botnets. Its goal is not to recover assets, but rather to disable the perpetrator's operation. Microsoft's tool of choice is a modern variety of civil litigation. Two features of civil litigation are particularly useful in this endeavor: 1) the use of subpoena power to uncover the computers in the botnet and the perpetrators that control it; and 2) the use of the court's power to issue an injunction that can a) sever the links between the "command and control" computers and the infected computers, b) allow Microsoft to inform the victim end-users that their computers are infected and provide them resources to remove the malware from their computers, and c) seize the "command and control"

computers under the theory that these machines are being used by the perpetrator to commit crimes including infringement of Microsoft's trademarks. A court has authority under the Trademark Act of 1984 as well as its broad equitable powers to order such a seizure to preserve the evidence for trial.[36] If the owner does not appear at the preliminary injunction hearing that would otherwise typically follow the issuance of the temporary restraining order, the preliminary relief can remain in place through the pendency of the case and ultimately remain in place through and following a default judgment process.

Because "botnet" architecture maintains multiple communications channels in anticipation of the possibility that any given link between individual computers will be severed, there are two key factors to effectively disable a "botnet": surprise and simultaneously severing all the links between the "command and control" computers and the infected computers.

Microsoft's experience taking down the Rustock botnet is illustrative. Microsoft obtained an under seal *ex parte* temporary restraining order directing all the domain registries and Internet Service Providers that housed equipment tied to particular domain names and IP addresses to unplug that equipment at a certain date and time. With respect to the domain registries and ISPs where there was concern the court order might not be timely followed, Microsoft enlisted the aid of the U.S. Marshal's Service to accompany Microsoft attorneys. Once on-site, they could ensure the order was followed and could seize the "command and control" computers as instrumentalities of the crime.[37]

While Microsoft was not able to recover any funds, that was not its goal. Its goal was to reduce spam, and it did; the Rustock takedown reduced global spam email traffic by 30% for several months following the takedown.[38] Though the effect may have been only temporary, Microsoft's goal—"disrupt, disrupt, disrupt"—was achieved.[39]

CONCLUSION

Significant thought is required to determine the appropriate tool to use against a perpetrator of cybercrime. The first thing to consider is whether to do a privileged investigation before proceeding. The answer to that question is almost always yes. A privileged investigation allows counsel to explore the facts as well as assess which of the tools at counsel's disposal may make sense.

Where counsel and client go from there is a complicated determination involving exploration of potential liability on the part of the client, identification of the perpetrator (or recognition that identification is impossible), investigation into the perpetrator's possible assets or items subject to seizure, and, crucially, the client's goals in pursuing the perpetrator. If traditional civil litigation may not be effective, other tools worthy of consideration include the modern civil lawsuit, the criminal referral, and the ITC complaint. In the Internet age, where cybercrime brings with it global reach and the threat of anonymity, it pays to consider alternatives to the traditional lawsuit, and to consider whether a modern civil lawsuit in the style of the botnet takedowns offers a client the best opportunity to reach into the Cloud to nab—or disable—a perpetrator.

NOTES

1. MODEL RULES OF PROF'L CONDUCT R. 4.1 (a) (2012).
2. CAL. BUS. & PROF. CODE § 6068(d) (Deering 2013).
3. *See* San Diego Cty. Bar Ass'n Opinion 2011-2 (2011) ("We have concluded that those rules bar an attorney from making an ex parte friend request of a represented party. An attorney's ex parte communication to a represented party intended to elicit information about the subject matter of the representation is impermissible no matter what words are used in the communication and no matter how that communication is transmitted to the represented party."); Phila. Bar Ass'n Prof'l Guidance Comm. Opinion 2009-02 (2009) (attorney may not direct a third party to "friend" a represented party for the purpose of gaining information to further a lawsuit).
4. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2012)).
5. *See* 18 U.S.C. § 2703. The Justice Department has recently announced that it considers the "180-day rule" outdated and wants to see it modernized. *The Electronic Communications Privacy Act ("ECPA"): Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary,* 113th Cong. (Mar. 19, 2013) (statement of Elana Tyrangiel, Acting Ass't Att'y Gen'l, Office of Legal Policy), available at *http://judiciary.house.gov/hearings/113th/03192013_2/Tyrangiel%2003192013.pdf*.
6. 18 U.S.C. § 2703.
7. *See* Memorandum from the Cong. Research Serv. on Legal Standard for Disclosure of Cell-Site Information (CSI) and Geolocation Information (to the S. Intelligence Comm. (June 29, 2010)), available at *http://www.fas.org/sgp/crs/intel/crs-csi.pdf*.
8. *See, e.g.*, Calif. Rules of Prof'l Conduct R. 5-100(A) ("A member shall not threaten to present criminal, administrative, or disciplinary charges to obtain an advantage in a civil dispute.") (2013).

9. CAL. PENAL CODE §§ 1377-1379 (Deering 2013).
10. *See* U.S. Attorney's Office, Cent. Dist. of Cal Press Release No. 10-003, West Hollywood Antiques Dealer Faces Charges of Selling Fake Picasso Drawing for $2 Million (Jan. 8, 2010).
11. Ted Johnson, 132 domain names seized in counterfeit ring: Move was part of crackdown on piracy tied to Cyber Monday, CHICAGO TRIBUNE (Nov. 26, 2012).
12. Office of Pub. Affairs, U.S. Dep't of Justice, 12-447, *Department of Justice Seizes More Than $896,000 in Proceeds from the Online Sale of Counterfeit Sports Apparel* (Apr. 10, 2012), available at *http://www.justice.gov/opa/pr/2012/April/12-crm-447.html*.
13. *Id.*
14. *See* United States v. Gupta, 2013 U.S. Dist. LEXIS 25594 (S.D.N.Y. Feb. 25, 2013).
15. *E.g.*, TEX. CODE CRIM. PROC. ANN. art. 56.43 (West 2013).
16. 19 U.S.C. § 1337(a) (2012);§ 1337(a)(1)(A). In addition, the authority explicitly includes semiconductor chip mask work registered under Chapter 9 of Title 17 and boat hull designs protected under Chapter 13 of Title 17. *Id.* at § 1337(a)(1)(D),(E).
17. *Id.* at § 1337(d)-(f).
18. *Id.* at § 1337(e).
19. *See* Sealed Air Corp. v. ITC, 645 F.2d 976, 985-86 (C.C.P.A. 1981).
20. *See generally* 19 C.F.R. §§ 210.27–210.34 (2012) (ITC Rules of Practice and Procedure, Subpart E—Discovery and Compulsory Process).
21. *See*, *e.g.*, U.S. Dep't of State, Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, available at *http://travel.state.gov/law/judicial/judicial_689.html*.
22. 19 U.S.C. § 1337(a)(1)(A).
23. An Economic View of the ITC's Domestic Industry, Law 360 (June 18, 2012).
24. *See generally* BRETT KINGSTONE, THE REAL WAR AGAINST AMERICA (2005).
25. Certain Robotic Toys and Components Thereof, Inv. No. 337-TA-869 (instituted 2013); Certain Paper Shredders, Certain Processes for Manufacturing or Relating to Same and Certain Products Containing Same and Certain Parts Thereof, Inv. No. 337-TA-863 (instituted 2012); Certain Rubber Resins and Processes for Manufacturing Same, Inv. No. 337-TA-849 (instituted 2012); Certain Electric Fireplaces, Components Thereof, Manuals for Same, Certain Processes For Manufacturing or Relating to Same and Certain Products Containing Same, Inv. Nos. 337-TA-791, 337-TA-826 (instituted 2011 and 2012, respectively); Certain DC-DC Controllers and Products Containing the Same, Inv. No. 337-TA-698 (instituted and completed 2010) (enforcement action instituted 2011 and completed 2012).
26. TianRui Group Co. v. ITC, 661 F.3d 1322 (Fed. Cir. 2011).
27. *Id.* at 1323-24.
28. *Id.* at 1335-37.
29. *See id.* at 1328-32.
30. *Id.* at 841.
31. *Id.* at 842-43.
32. C.S.B. Commodities, Inc. v. Urban Trend (HK) Ltd., 626 F. Supp. 2d 837, 841 (N.D. Ill. 2009).
33. *Id.* at 853-56. The court did find personal jurisdiction over the president of Urban Trend, a resident of Hong Kong, because he was personally served in Illinois. *See id.* at 841, 845-47.
34. Certain Lighters, Inv. No. 337-TA-575, USITC Pub. 4112 (Nov. 2009) (Final).
35. Certain Handbags, Luggage, Accessories, and Packing Thereof, Inv. No. 337-TA-754, USITC Pub. 4387 (Mar. 2013) (Final).
36. *See* Trademark Counterfeiting Act of 1984, Pub. L. No. 98-473, Tit. II, § 1502(a), 98 Stat. 2178.
37. For a similar case with extensive pleadings and orders available for review, see Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, Microsoft Corp. v. John Does 1-18, Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers, Case No. 1:13 cv 139 (E.D. Va. Jan. 31, 2013), available at *http://www.noticeofpleadings.com*. Microsoft's brief in support of the temporary restraining order and the court's corresponding ruling are full of compelling details that reveal how botnets work and how to disable them.
38. In March 2011, a Microsoft team took down the Rustock botnet; the decrease in spam was immediate and dramatic. As of April 2012, spam levels had still not recovered. Spam levels were at 150 billion just before the takedown; as of the first quarter of 2012, levels were at an average of 94 billion. Jon Brodkin, *Spam levels still low a year after Rustock botnet takedown*, ARS TECHNICA (Apr. 5, 2012), *http://arstechnica.com/business/2012/04/spam-levels-still-low-a-year-after-rustock-botnet-takedown/*.
39. Nick Wingfield and Nicole Perlroth, *Microsoft Raids Tackle Internet Crime*, N.Y. TIMES, March 26, 2012.