

Receiverships and Other Shark Tales

by Dana J. Lesemann and Peter B. Zlotnick

“Put down the phone and step away from the computer!” The telemarketer stares at the suited man accompanied by a team of uniformed police officers, attorneys, and investigators from the Federal Trade Commission, plus accountants and forensic computer specialists toting briefcases and equipment. The “raid team” has suddenly appeared in front of her cubicle.

She’s wearing a headset and sitting at a paper-strewn desk topped with a computer. Seconds earlier she had been talking to a customer, reading from a script on a monitor in front of her and recording information into a central database. Behind her are at least a hundred people doing exactly the same thing in a cubicle-filled boiler room.

The man in the suit steps into the center of the room. “Ladies and gentlemen, please put down your telephones and move away from the computers. I’ve been appointed temporary receiver of Sink or Swim Credit Repair by the federal district court, and this business is closed for today.”

The receiver directs each of the employees to move to the front of the room, where he will take down their names, addresses, telephone numbers, and Social Security numbers (some real, some fake). He also will note information about their jobs at the company and to whom they report, creating an organizational chart. The receiver’s team moves through the offices with digital cameras, photographing and inventorying the premises.

Out of the corner of his eye, the receiver sees a young man start to slip something the size of a hardcover book into his briefcase and slink toward the front door. “Excuse me, sir,” the receiver says. “What’s your name?”

“I just do some accounting for the company,” the young man says, glancing around furtively. “I don’t even work here. I’ve got another appointment. I’m outta here.”

“Your name, sir,” the receiver demands.

“Don Jackel,” the man answers reluctantly.

The receiver continues the interrogation: “What was that you put in your briefcase?”

“That’s my personal computer equipment,” insists the young man. “I did some work for Sink or Swim on it, but it has lots of other accounting information on it that I did for other companies, too. But it’s mine, not the company’s.”

“Mr. Jackel, under the terms of the Temporary Restraining Order issued by the court, I need to take possession of *all* of Sink or Swim’s books and records,” asserts the receiver. “As soon as I can, I will make a forensic copy of the information on your equipment and, if I can, I will return it to you.”

Jackel reluctantly hands over the external hard drive—which in fact contains all of the company’s financial records.

The door to a back room flings open, and a man in his mid-30s hurries out, wearing a Rolex watch of questionable origin, a diamond pinkie ring, and a thick gold chain around his neck. He reeks of too much cologne. The receiver asks if he is John Sullivan. “Who wants to know?” the man asks. One of the FTC investigators pulls out a driver’s license picture of Sullivan. “Yes,” the investigator confirms, “that’s him.”

The receiver wants to be sure. “Are you John Sullivan? Are you the owner of Sink or Swim?”

“Yeah, the girl’s right. That’s me. What’s it to you?”

The receiver introduces himself while one of the police officers serves Sullivan with a copy of the court papers: a complaint filed by the FTC under Section 5(a) of the Federal Trade Commission Act (FTC Act), alleging, among other things, that Sink or Swim has defrauded consumers by deceptively marketing a program to assist consumers in consolidating their credit and debit card loan obligations; a temporary restraining order appointing the receiver and freezing Sullivan’s personal assets and the assets of Sink or Swim; and a six-inch-deep pile of exhibits containing evidence of the FTC’s case—including statements from two former Sink or Swim employees, a transcript of a call with Sink or Swim made by an FTC investigator, and statements from 15 alleged victims who say they were scammed by Sink or Swim.

The receiver tells Sullivan that he has not been found liable for any wrongdoing. He explains that the receiver’s role is to marshal, preserve, and protect Sink or Swim’s assets until the court either dissolves the receivership or the FTC’s lawsuit is completed with a final judgment entered in favor of one of the parties. The receiver is an appointee of the court and, he tells Sullivan, is not an agent of the FTC or involved in the lawsuit. He is neutral and owes fiduciary obligations to the corporate estate.

“Right,” Sullivan spits. “That’s why you came here with those jack-booted thugs.”

“Mr. Sullivan,” the receiver patiently replies, “I’m simply here to uncover the facts and report them to the court. It’s in your best interest to cooperate with me. You need to understand that the court has frozen your personal assets and the assets of the corporation. I have the right, indeed the obligation, to go through every nook and cranny of this business to find out what has been going on and how you have operated this company. I will be investigating whether I think any fraudulent conduct has occurred here. For that reason, you would do best to get yourself a lawyer.”

Having the false bravado and confidence of . . . well, a confidence man, Sullivan fails to take the receiver’s advice. Ignoring the court’s order directing him to refrain from interfering with the receiver’s activities, Sink or Swim’s president jumps on top of a desk and motions for his staff to gather

Dana J. Lesemann is with Stroz Friedberg, LLC, a computer forensics consulting firm in Washington, D.C. Peter B. Zlotnick is with Mintz Levin Cohn Ferris Glovsky & Popeo, P.C., in New York City. The authors thank their friends and colleagues at the Federal Trade Commission, especially Steve Gurwitz, for their time and assistance with this article.

round. He tells them, “Don’t worry, everyone. We’ll be back up and running tomorrow morning, business as usual. This doesn’t change anything. Meet me at Sal’s Bar and Grill in an hour and we’ll talk about next steps. And I guarantee that each one of you will get paid every cent that is owed to you.”

As the words leave Sullivan’s mouth, one of the uniformed police officers moves in. “Get down, Mr. Sullivan. You have until the count of three or you will be coming to central booking with us. One . . .” Sullivan’s arrogance melts away. His shoulders droop and he slinks down off the table. Then he catches his sales manager’s eye and, with an almost imperceptible nod, acknowledges his friend. Sullivan looks contrite, announces that he has to use the men’s room, and heads toward the back of the office where the restrooms are located—and where, more importantly, the business’s computer servers are.

And, thus, a typical FTC receivership begins.

Receiverships are the FTC’s way to shut down scams, using court-appointed receivers to marshal assets and to identify, preserve, analyze, and forensically copy electronic information to develop evidence of fraud. Each receivership has its own story, and each story has important lessons for all litigators—not just those litigating with the FTC or agencies with similar authority such as the Securities and Exchange Commission (SEC) or the Commodities Futures Trading Commission (CFTC). Even litigators dealing with bankruptcy fraud or electronic discovery outside the context of regulatory agencies can learn from receivership stories.

Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits any “unfair or deceptive act or practice” in or affecting commerce. Section 13(b) of the Act, 15 U.S.C. § 53(b), allows FTC attorneys to go directly to federal courts for injunctive relief. They have done so frequently, shutting down fraudulent enterprises using ex parte temporary restraining orders obtained under Rule 65(b) of the Federal Rules of Civil Procedure. For an overview of how the FTC came to use its power under Section 13(b), see David Spiegel, “Chasing the Chameleons: History and Development of the FTC’s 13(b) Fraud Program,” 18 *Antitrust* 43 (Summer 2004). The FTC’s power under Section 13(b) is similar to the SEC’s and CFTC’s authority under their respective enabling legislations. These agencies can also obtain orders under Rule 65(b), which enables federal courts to issue TROs ex parte—without written or oral notice to the adverse party—if “it clearly appears from specific facts shown by affidavit or by the verified complaint that immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or that party’s attorney can be heard in opposition” and the attorney certifies “the reasons supporting the claim that notice should not be required.”

A typical temporary restraining order appointing a receiver runs 20 to 25 pages. In contrast to a bankruptcy or statutory real estate receivership, which is constrained by code or rule, this type of FTC action results in an appointed equity receivership that has all of the powers of that court. The receiver is appointed for the initial TRO period to maintain the status quo, after which the receivership is dissolved or maintained until the case is resolved.

TROs generally enjoin the defendants from making misrepresentations and material omissions or providing others with the means and instrumentalities to violate Section 5 of the FTC Act. Many computer-savvy scam artists set up shop on the Internet. Receivers and the forensic examiners who

work with them have to be equally knowledgeable, and the court orders also have to keep pace. Thus, a typical TRO will now prohibit defendants from hosting, operating, or destroying any Internet web pages or websites. The receiver’s team also must monitor the defendants’ activities in order to ensure that they are in compliance with the court’s order.

A standard TRO appoints the receiver to take control of all corporate defendants, as well as any subsidiaries or affiliates that are owned or controlled by the principals of the receivership, who usually are the individual defendants. This broad mandate often raises questions at the outset of a case as to which companies fall within the sphere of the receivership, particularly when the receiver’s team finds other businesses operating in the same space leased by the defendants. By examining the bank accounts, general ledgers, leases, and corporate records of the companies, the receiver usually can rapidly resolve any issues relating to the interrelationship of the affiliates, as allowed under the TRO.

The TRO gives the receiver access to all of the defendants’ business premises and any other location containing the business records. The order requires the defendants to turn over all funds, property, books, records, keys, entry codes, and combinations to locks required to open or gain access to any property, as well as information identifying the accounts, employees, properties, or other assets or obligations. In addition, the defendants must provide the receiver with computer passwords necessary to access all business data.

TROs typically include asset freezes that prohibit the defendants from using any funds—wherever located—and require the repatriation of any assets located in foreign countries. The defendants are required to provide the FTC and receiver with sworn financial disclosure statements within a short period of time, and to appear for asset depositions should the receiver or the FTC require. Invariably, the TRO directs all third parties served with the TRO to deliver any funds or property of the receivership companies to the receiver upon written request.

The defendants must provide a copy of the order to anyone who works for them. The TRO remains in effect for no more than ten days, while the receiver and his team act to identify and secure the electronic and physical records of the companies and to locate and freeze assets. When this ten-day frenzy ends, the court holds a preliminary injunction hearing and decides whether to dissolve or maintain the receivership until the litigation is resolved.

The primary responsibilities of the receiver are to preserve the status quo pending resolution of the case and to report to the court on the nature of the defendants’ business. Although receivers are neutral parties and are not arms of the FTC (or other enforcement agency), defendants almost always perceive them as enemies who are interfering with their property and privacy rights. As a result, defendants frequently obstruct the receiver or refuse to comply in one way or another.

In one memorable case in the late 1990s, four days after the service of a TRO on the principals in a pyramid scheme, one of the consumers alerted the receiver that the defendants had resurrected their enjoined scheme on a new website. According to the consumer, the defendants even were holding weekly conference calls with the same program participants they had been soliciting before the receiver took over the companies. The receiver confirmed the report and notified the defen-

dants' counsel that his clients were violating the TRO's requirements. Within hours the defendants shut down the website and stopped the conference calls, but the stage had been set for a contentious relationship.

Obviously, once the FTC has obtained a temporary restraining order, it has made a compelling case that it will prevail on the merits. The possibility always exists, however, that the agency and the court are wrong and the defendants have not

Defendants almost always perceive receivers as enemies.

violated the law. The receiver's responsibility is to preserve the property for the ultimate prevailing party—whoever that may be.

Because of these conflicting demands, the receiver's job is not easy. From the moment he walks in the door of a boiler room, he is viewed as the enemy. In order to prove that he is neutral, he may have to risk alienating the agency that, in all likelihood, suggested him as the court-appointed receiver. If he was not suggested by the agency, he may have been thrust upon an unwilling FTC—leaving both of them unsettled with the arrangement. Either way, he likely will have few friends on the premises.

In one case, a receiver interviewed a defendant in a crowded one-room storefront in the presence of two uniformed police officers. Throughout the interview, the defendant shifted in his seat and responded nervously to the receiver's questions. The defendant asked if he could use the bathroom. The receiver agreed. Luckily for the receiver and everyone else in the room, the police officers were exceptionally thorough. Before the defendant could take one step toward the bathroom, one officer held up a hand and the other moved swiftly into the bathroom to inspect it. Moments later he reappeared, holding a large, serrated hunting knife by two fingers of one hand and a semi-automatic handgun with a laser site with two fingers of the other. The firearm was unregistered. As a result, the defendant's evening quickly degenerated from a simple receivership into a more serious matter.

This type of welcome mat, however, presents special challenges to a receiver, especially after the recent shooting in Chicago of a federal judge's husband and mother. Once the police secure the premises and leave the site, however, the risks do not necessarily diminish. Even after the professionals hired by the receiver change all the locks and shut down all computer servers, defendants come up with imaginative evasive actions—some dangerous, some devious. Without fail, much of any receiver's time will involve solving the "crisis du jour" created by a recalcitrant defendant who conceals a fraudulent insurance claim of lost receivership property without disclosing it.

For this work, the receiver is entitled to reasonable compensation, generally from the assets marshaled into the estate. Sometimes he makes money, sometimes he barely covers expenses, and sometimes he ends up meeting his pro bono obligations for the year in one go. That is the financial

risk the receiver and his professionals accept at the outset of each receivership.

In the early days of litigation under Section 13(b) of the FTC Act, the scope of the receiver's power was not well defined. In one case in the late 1980s, a defendant tried to take a Federal Express envelope from a business under receivership. When challenged by the receiver, he claimed that it was personal property and not part of the business, and insisted on taking the envelope. The receiver relented. It turned out that the envelope contained a key to the defendant's safe deposit box. By the time the receiver obtained a court order to get access to the safe deposit box, the box was empty. These days, most receivers would not hesitate to insist on taking possession of the envelope, or anything else found on the defendant's business premises, and, if necessary, to call on law enforcement to enforce the TRO.

Over time, though, defendants have become more creative in finding ways to hide assets. In terms of both obstinacy and sheer gall, few defendants can hold a candle to Ken Taves, who ran what the court euphemistically called "adult-content websites." On January 6, 1999, a court issued a TRO, froze the assets of Taves and his wife, and appointed a temporary receiver to administer the defendants' businesses. Laptop computers that had disappeared from the business reappeared, mysteriously scrubbed of all data. In May 1999, the court held Taves in contempt for failing to disclose a Malibu estate that he transferred to a corporation a month after the TRO was issued. The court ordered him to pay the receivership \$2.5 million, the estimated sale price of the property. Taves then tried to move money from an account in the Cayman Islands to pay the \$2.5 million owed. Taves, however, had failed to disclose to the receiver the existence of that account, which contained \$6.2 million in cash and securities—another violation of the TRO. Taves and his wife were ordered to repatriate the money and again were held in contempt. This time, Taves was placed in the Los Angeles Metropolitan Detention Center and later was convicted of criminal charges associated with the underlying fraud. *See FTC v. J.K. Publications*, 99 F. Supp. 2d 1176 (C.D. Cal. 2000).

As defendants have become more creative with hiding assets, receivers have learned to be creative to ensure that justice is done for consumers. In one of the FTC's earliest cases filed under Section 13(b), *FTC v. U.S. Oil & Gas*, 1987 U.S. Dist. LEXIS 16137 (S.D. Fla. 1987), receiver Gerald Wald convinced the court to allow him to file a class action suit against almost 100 banks, insurance companies, law firms, and other defendants on behalf of the victims of an investment scam, alleging securities fraud and RICO violations. The defendants entered into major settlements with the plaintiffs, recovering almost \$50 million in lost investments. Other receivers, however, have not been successful in convincing courts to allow them to institute suits on behalf of individual consumers since, in reality, the receivers represent the corporation.

In the early 1990s the FTC brought a lawsuit against Metropolitan Communications, which defrauded thousands of victims in the sale of FCC wireless licenses. The authors of this article were involved on behalf of the FTC and as receiver's counsel. The court-appointed receiver, Daniel Goodman, spent years litigating with and lobbying the FCC to allow the licensees to assign the licenses to Nextel and other companies.

The problem was that each consumer's license either had expired or was about to lapse. The FCC at first refused to grant any extensions to the defrauded consumers, but, thanks to the persistence of Goodman and his team, the agency eventually relented. For the first time in its history, the FCC issued a rule granting an extension of time for all the consumers, even those whose licenses had expired. As a result, the consumers recovered almost all their investments.

All receiverships are not, however, made in heaven. One FTC attorney was concerned by a receiver's consistently late reports and continued to press him for detailed information about the estate. Finally, the FTC attorney got a call from a criminal defense lawyer who represented the receiver. It turned out that the receiver had been embezzling from a number of parties over the years, including FTC receiverships, bankruptcy trusteeships, and other estates. In a classic Ponzi-type scheme, he had shifted assets from one estate to another to cover up the fact that he was using the assets for his own gain. The receiver died before criminal charges came to fruition, but it was a painful lesson for the FTC in dealing with receivers.

In addition to finding the money, the receiver has to report to the court about how the business was run, including the nature of the business, the amount of money it brought in, the number of consumers allegedly injured, and the role of the defendants and any other officers and directors. The first step in this assignment is interviewing all the decision makers and managers of the company to determine how they operated the company on a day-to-day basis. And, although the TRO requires the defendants to provide the receiver with all books and records, telemarketers are not renowned for their record-keeping abilities. As a result, the receiver often has to re-create much of the information from the defendants' computers.

This is another concern for the computer forensic expert, who must preserve and authenticate the data; recover information that may be encrypted, password protected, deleted, partially overwritten, or otherwise unavailable to everyday users; and make the data available in a useful form for the receiver and the FTC. The examiner has to know to look wherever electronic data can be stored—desktop and laptop machines, servers, PDAs, handheld communication devices, thumb drives, digital cameras—all of which can provide a gold mine of evidence that can shed light on how a business was conducted, who was in the inner circle, who the victims were, and where the money went. Once the data is forensically preserved and forensically copied, the computer expert can be prepared to authenticate it should the matter ever be challenged in court.

But data on computers is fragile. The receiver's initial command—"Put down the phone and move away from the computer"—is more than melodrama. The simple act of turning a computer on or off can destroy the very evidence you may want or need. In most cases, computers write files to the hard drive in the process of booting up. These files could overwrite previously deleted material that could otherwise have been recovered and may have been relevant to the investigation. In addition, operating systems may be configured to trigger certain functions on boot-up, which also may affect the investigation. For example, if the question arises as to when a defendant looked at certain computer-stored memos, booting up may trig-

ger a virus scan that touches each active file and changes the last access dates for those memos. On the other hand, computer memories can contain crucial evidence that can be lost if the computer is turned off. So the key rule is: If the computer is off, leave it off; if the computer is on, leave it on.

Files stored on more recent versions of the Windows operating system have three critical bits of information, called "metadata," that reveal when a file was created, was last modified, and was most recently accessed. Some word processing and e-mail programs also contain additional metadata that include the author's name, text revisions, and names of people who made changes to a document. In addition, even if a document was not saved to the hard drive, there may still be a record of it that forensic experts can recover. If someone printed it, a temporary file exists until it is overwritten.

If a defendant claims ignorance of a specific document, evidence that the document was opened, edited, or saved may exist on her computer. For example, the recent Nigerian Barge Case brought by the Enron Task Force centered on the sham sale of a \$7 million Nigerian oil barge from Enron to Merrill Lynch, which Enron booked as revenue. Forensic experts searched the company's computers for electronic copies of a

Turning a computer on or off can destroy the very evidence you need.

memo in which the barge transaction was characterized as a loan, not a sale. They identified and preserved an electronic copy of the incriminating memo in the home directory of one of the indicted Merrill executives, who claimed that he had never read it. The expert, however, explained to the jury that the executive had likely received the document via e-mail and saved the document to his home directory after editing it. The executive was convicted.

Hard drives can hold millions of pages of files and present an overwhelming volume of information. A 20-gigabyte laptop, for example, holds the equivalent of 5.2 million pages of paper; a 40-gigabyte desk top hard drive—not small, but by no means the largest size on the market—holds the equivalent of about 10.5 million pages of paper. You would need two semitrucks to cart away that amount of paper. A forensic examiner can work with the receiver to develop a list of keywords that will identify even deleted and partially overwritten documents that may still exist—and that may contain such terms as "guaranteed returns," "no risk," and "100 percent." For any scam, the phrase "easy money" is another red flag. Instead of looking for a specific keyword, a search utility called GREP (generalized regular expression parser) identifies all telephone numbers, Social Security numbers, and e-mail addresses or physical street addresses that may be on the hard drive, which is valuable for locating former employees, storage facilities, or other boiler rooms.

In a telemarketing operation, key information about the business lies in the scripts: what they say, and who wrote, edited, and circulated them. In the mid-1990s, receivers' teams looked

for photocopied scripts with handwritten comments, and deposited salespeople to find out who handled the scripts. These days, forensic examiners can go to the company's computers and find "Wayne's Winning Sales Script" on the hard drive. Further forensic study can unearth the following evidence:

- Metadata that demonstrated that Wayne created the document on January 1, 2005, and included the original promise of a "guaranteed 1,000 percent return on investment within

For any scam, the phrase "easy money" is another red flag.

30 days with ABSOLUTELY NO RISK."

- Evidence that Wayne e-mailed the document to the entire telemarketing staff with this message: "Use this script to front investors. You must follow it exactly. Talk to me or Joan or Deanna if you have any questions."
- A document history that shows Joan edited the document on January 10, 2005, added the words "AND YOU CANNOT LOSE YOUR INVESTMENT!!" to the script, and e-mailed it to the telemarketing staff with the following message: "Staff!! Some of you are not SELLING HARD ENOUGH. YOU KNOW WHO YOU ARE!! WE *MUST* DO BETTER! Here is the new script."
- Another edit Deanna made to the script on January 12, 2005, changing "1,000 percent return" to "1,500 percent return," and sent to Wayne and Joan with an e-mail message that said, "Do you think this will help increase sales? I'm not sure what else we can change to get people to buy this garbage."

Deanna, Joan, and Wayne can later deny that they had any managerial control over the scam, but the metadata on the documents and the associated e-mails show their editorial control of the script, which demonstrates that they had some level of authority. Handwriting analysis might provide further proof if handwritten changes to the scripts are part of the evidence. But the defendants will be hard-pressed to argue that someone stole their passwords to create or edit a script, especially when it is accompanied by other incriminating e-mails.

As we all now know, when a file on a computer is deleted, it is not really gone. The computer simply removes its reference to that file, effectively forgetting where the associated data is located on the disk. However, the data still exist until overwritten by new data. Forensic examiners therefore may be able to recover part or all of a deleted file, provided that it has not been replaced with new data. In addition, fragments of a deleted file may even be recoverable if the original file is partially overwritten. When a new file is saved to the disk but is smaller than the one it replaces, forensic examiners will be able to recover remnants of the old, larger document. Imagine that a large document called "Wayne's Winning Sales Script" was deleted from the defendant's computer, and a smaller document called "Wendy's Even Better Sales Script" was

saved to that same area of the drive. A forensic examiner may be able to find fragments of Wayne's script—the earlier, bigger version—under Wendy's script. However, the more frequently new data is saved to the hard drive and the longer a computer is in use, the more likely it is that old, deleted data will be overwritten.

Forensic experts can create a library of hash values for brochures, scripts, and sucker lists that have been passed from scam to scam, then search target computers for those hash values. FTC orders often ban defendants from selling or otherwise transferring their customer lists; creating a hash library could provide important evidence of violations of federal court orders. The use of brochures and scripts from scams previously targeted by the FTC or other agencies is evidence that the defendants knew full well that they were engaged in fraud.

Sometimes defendants use public key encryption such as PGP (Pretty Good Privacy) or another program to encrypt e-mail or other data on hard drives. To read each other's encrypted e-mail or documents, each person needs the other's public key, which creates what PGP calls a "web of trust." Even if the communications or documents have been encrypted for the computer, experienced forensic experts have tools and methodologies to locate plain-text versions of some of this data. Telemarketing operations also often have "front people" who appear to run the business while the real powers hide behind the scam. The "money men" do not want their names on any of the paperwork, but they may want the ability to check on the business. To keep their hands in the operation, they sometimes insist on access to encrypted e-mails or documents. Find the money man's private key to access the business's encrypted files, and he becomes a co-conspirator.

A receiver's potent weapon for securing the status quo—the 20-some-page order issued by a federal district court that gives the receiver extraordinary power to marshal assets, take depositions, and examine every nook and cranny of a business—packs a heavy wallop. The power of that punch has become even greater with the use of forensic computer experts to identify the defendants' electronic media; to find deleted, encrypted, and password-protected files; and to recreate the databases defendants used to store information about their victims. But always remember the receiver's first rule for preserving electronic evidence: When you burst through the defendants' door, always announce that it's time to put down the phone and step away from the computer. □