Antitrust, Vol. 22, No. 1, Fall 2007. © 2007 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

The Criminalization of Consumer Protection—A Brave New World for Defense Counsel

BY BARRY J. CUTLER

Prologue

Great excitement was brewing in consumer protection circles one lunch hour at the end of March 1993. FBI Director William Sessions had scheduled a 2:00 p.m. press conference to unveil the FBI's ambitious new program to combat telemarketing fraud. Exhibits of health fraud, business opportunity fraud, and other varieties dotted the auditorium where a packed audience, including media, were expected in less than an hour. It was a satisfying moment for consumer protection law enforcers who long had felt that the FTC and other "civil" law enforcement agencies were fighting an uphill battle to prosecute essentially criminal cases with the often inadequate tools of access letters and cease and desist orders. The belated, but welcomed, arrival of the Department of Justice on the scene meant both that the government would be able to "fight fire with fire" and that the FTC and other agencies would have an ally to seek criminal remedies in appropriate cases.

As the minutes ticked down to 2:00 p.m., there was an obvious delay but no immediate hint of the cause. Came 2:30 p.m. without sign of the FBI Director or the Acting Attorney General. The packed auditorium was filled with circulating rumors, but no confirmations. In due course, the Director and the General entered and made their way to the podium, where the Director announced the arrests at 12:30 p.m. of three suspects in the 1993 bombing of the World Trade Center in New York City, which had occurred weeks earlier. He also made some brief comments about telemarketing fraud. During the frenzied question and answer period that followed, there was not a single question about telemarketing fraud. Nor did the topic draw any notable media attention the next day.

Like many watershed moments, the true significance of this one was not fully appreciated at the time. Law enforcers struggled on with civil cases, referring occasional criminal cases for violations of federal court orders. A full decade passed before a formal liaison with the Department of Justice was created in 2003.

The terrorism that stalled the DOJ telemarketing initiative in 1993 may now bring it closer to fruition in the context of the Web. A July 6, 2007, headline on page one of the Business Section of *The Washington Post* read: "Three Worked the Web to Help Terrorists," followed by the subheadline "British Case Reveals How Stolen Credit Card Data Bought Supplies for Operatives." Those annoying requests to verify e-Bay account information are, according to the article, not just for routine hackers, but for networks of worldwide terrorism as well. "Investigators in the United States and abroad spent hundreds of hours tracking the financial activities of [the three alleged suspects] across thousands of merchants in more than a dozen countries." The linkage of terrorism and consumer fraud has come nearly full circle.

Overview

In the last fifteen years, the FTC has been forced to investigate and litigate more and more matters that could have been better handled as criminal frauds under 18 U.S.C. § 1341 (mail fraud), § 1343 (wire fraud), and other criminal provisions. Playing "the cop on the beat" to maintain high standards among national advertisers largely has given way to efforts at recovering money for defrauded consumers and addressing online security and privacy breaches. One sees fewer household names in advertising and other cases brought to maintain fair competition, but more "operations," "projects," and "sweeps" that produce larger numbers of cases of lesser competitive significance—the companies and individuals bound by permanent injunctions being quickly replaced by new actors using similar practices. The fact that the Internet is worldwide will make it increasingly difficult for the FTC to identify, prosecute, and punish bad actors who, like the terrorists impersonating e-Bay, may be scattered around the world.

The changing face of consumer protection enforcement, as seen in the FTC's annual reports since 1990, seems not to be a matter of the Commission's own choosing. In the years since the aborted telemarketing fraud press conference, actions to curb identity theft, privacy abuses, and serious frauds increasingly fell upon the FTC by default. The FBI and Department of Justice had more urgent security priorities. The U.S. Postal Inspection Service, which had done fine criminal work in the years when use of the U.S. mails

Barry J. Cutler is a partner in the Washington, D.C. office of Baker & Hostetler LLP. He previously served as an Assistant U.S. Attorney (Connecticut) from 1970–1974, as a Deputy Assistant Director and Assistant General Counsel of the FTC from 1974–1978, and as Director of the FTC's Bureau of Consumer Protection from 1990–1993. He has been involved in the prosecution or defense of several of the matters referenced in this article. *The research efforts of Jessica Batzell are gratefully acknowledged.*

provided its federal jurisdiction, became less effective as the Internet and emails largely replaced the U.S. mail as favored vehicles for fraudulent activity.

These shifting enforcement priorities have substantially changed the traditional role of the FTC consumer protection bar, introducing key elements of criminal law and procedure into the private practice of consumer protection law. Concerns about fee arrangements abound. Legal and ethical questions about advising clients regarding potential criminal exposure and the use of Fifth Amendment privilege arise more frequently than analysis of copy tests about ad meaning or the interpretation of complex credit statutes. This article describes some of these challenging questions and provides some practice tips for dealing with the criminal aspects of consumer protection law practice.

The New Frontier of Consumer Protection

One way to measure the changing mix of consumer protection activities is to analyze consumer complaints. According to the FTC's most recent report,[1] the biggest consumer complaint by far involved identity theft (48%), along with Internet services (8%), Internet auctions (6%), and foreign money offers (4%). Even without counting other categories that may have Internet elements, it is clear that at least two-thirds of the complaints received by the FTC involved fraudulent and deceptive practices that did not even exist in 1992. That percentage has been growing steadily in the last several years, according to the annual FTC Reports. From the mix of consumer complaints, reflected in the changing composition of consumer enforcement efforts, flow some important consequences.

First, it has become increasingly hard to learn some of the basic details of a scam, including who is doing it, where they are located, and how much they are making. The Internet affords a type of anonymity that we have not seen in more than a century, when slick salesmen made live pitches, took cash, and got out of town. In the decades that followed, whether through mail order, direct radio and TV, or telemarketing, there usually was a paper trail of check routing, credit card processing, and P.O. Box numbers and addresses that made it easier to get on the trail of con artists and their support networks. With the advent of a the World Wide Web, online transactions, and identity theft, it may still be possible—though with much greater effort and more sophisticated investigatory techniques—to "follow the money" and get some information about the wrongdoing. However, voluntary requests for information and cease and desist orders hardly seem adequate to rein in recidivists who engage in hard core consumer fraud.

For its first eighty years, the FTC typically ignored the scams advertised in supermarket tabloids, concentrating instead on national advertisers and high impact cases that would provide clear guidance to marketers about the standards that were expected in a competitive marketplace. That enforcement strategy made sense at a time, prior to the mid-1990s, when there was no Internet or Spam, and tabloid scams rarely reached broadcast or mainstream print media.

Fast forward a decade and consider the challenge of an FTC "Surf Day" in which the FTC staff searches the Internet for health care frauds, phony business opportunities, and the like. "Locking in" on a particular Web site, unlike following direct mail or broadcast advertising, provides little insight into whether an apparently fraudulent site represents a $50 million operation or a few guys in a garage who, prior to the Internet, might have advertised in the supermarket tabloid. The result is many more investigations against small time crooks.

Even when enforcers negotiate the maze of telephone switches, spoof emails, and credit card laundering to find out "where" a scam is based, there is little assurance that it will be where the FTC can invoke its own enforcement jurisdiction or secure the cooperation of host countries. Although international coordination has improved in recent years, this effort has been, and remains, a daunting task for dealing with scams that can move around the world. In some ways, today's challenge is more akin to chasing the con artists of the 19th century than it is to tracking down those who used direct marketing and telemarketing in the 20th century. The natural result of all of this, it would appear, has been an inevitable rise in the number of small impact cases with little effect on changing marketplace practices and a corresponding reduction of resources available for the FTC's more traditional role as referee of a working, competitive marketplace.

One way to measure the effectiveness of current enforcement is to ask whether more credit repair cases have led to less credit repair fraud; or whether more identify theft and data security cases have led to less ID theft and computer hacking; or whether more cases of advertising work-at-home and other schemes have reduced abuses in those areas. The listing of "top ten complaints" in the last several FTC annual reports suggests that the answer is a resounding "no." No finger-pointing is intended here. Unless federal criminal authorities can shift more attention and resources to criminal-type consumer frauds, the FTC seems destined to remain the federal agency of last resort.

A second effect of the shift toward more hard-core fraud cases has been the Commission's perception of appropriate relief in individual cases. By the late 1990s, a group of tough-minded Commissioners pushed harder and harder for complete consumer redress, at least to the extent that funds could be located and seized. They also presumed that staff would name key individuals in closely held companies unless there was a compelling reason to the contrary. Neither the FTC staff nor the consumer protection defense bar could fail to recognize the new emphasis on enhanced remedies.

Even this "give it all back" approach, however, could take enforcement efforts just so far. When money was either spent or hidden around the world, finding all of the money in the defendant's own hands was unlikely. Total returns of significant sums were more the exception than the rule. The

FTC followed a "dandelion" theory to go after the "root systems" that benefited from assisting frauds. In the early 1990s, for example, the FTC achieved a $47 million redress fund thanks to an assertive receiver who challenged banks, lawyers, accountants, and insurance companies that had facilitated or at least turned a blind eye to the operations they were helping.[2]

Today's Internet frauds are not likely to be abetted by large banks, accountants, lawyers, and insurance companies. Full redress for consumers is the exception rather than the rule. Instead of "dandelions," the FTC has turned to what one FTC defense lawyer calls the enforcement equivalent of "Whack-a-Mole." Shutting down companies and individuals through asset freezes and TROs or parallel indictments and criminal prosecutions has been a higher priority in many cases than trying to rehabilitate them through permanent injunctions. The FTC's focus creates the need for FTC defense counsel increasingly to be concerned about the added elements of criminal risk in FTC cases.

The FTC and Criminal Enforcement

FTC involvement in parallel criminal matters is not new. An FTC Regional Office circa 1972 referred an aluminum siding company to the U.S. Attorney's Office in Connecticut for what was believed to be the first criminal prosecution in the country under the recently enacted Truth-in-Lending Act. The FTC has handled cases over the years involving magnetic gas mileage improvement devices that were also the subject of mail fraud prosecutions in New York and Connecticut. And at least two FTC cases against rare coin dealers have resulted in criminal convictions.

Still, it was startling in the 1970s to see how rarely a potential FTC respondent would "take Five" (assert a Fifth Amendment privilege), even as the FTC brought cases with criminal potential, including certain business-to-business scams that had the hallmarks of organized crime activities. From the early 1970s to the early 1990s, a few FTC matters turned criminal, but these isolated "bolts of lightening" did not provoke much concern among the FTC defense bar.

In the 1990s, as the FTC's use of Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), for civil frauds was stepped up, there was a general increase in the number of criminal cases that grew out of FTC civil proceedings. The great majority of these involved criminal contempt of federal court orders, either violations of preliminary asset freeze orders or continuing conduct in violation of a permanent injunction.

By 1996, only three years after the 1993 FBI press conference, FTC enforcement took two important turns. First, the FTC announced "Project Scofflaw" to highlight the use of criminal enforcement for serious violations of federal court orders. Working in an organized fashion to ferret out such violations, the FTC triggered at least thirty-six criminal cases between 1997 and 2006. The effort continues today.

Parallel to this studied increase in "Scofflaw" cases was a mushrooming of civil fraud cases that, for the first time, involved either Internet advertising or direct e-mail solicitation. These included the Commission's first case against a big Internet pyramid scheme (1996), a "Field of Schemes" project for fraudulent online investments (1997), "Project Net Opp" for Internet business opportunity scams (1998), and (how can we ever forget) phony Y2K schemes (1999), among many others. The FTC's annual reports during this time period provide ample proof of how the new electronic age was creating a "Brave New World" of consumer protection.

For defense lawyers engaged in counseling or litigation for FTC respondents, the risk of potential criminal liability for violations of court orders should not have been a surprise. "Project Scofflaw" was designed with the specific purpose of enhancing the credibility and force of a Commission or federal court order. The party violating an existing order would be poorly advised if left to believe that violations of outstanding administrative and court orders could result in no more than a slap on the wrist.

Concern about parallel criminal actions in the first instance was another matter. Evidence of increasing criminal risk was made manifest in 2003 by the FTC's announcement of a Criminal Liaison Unit (CLU). According to the FTC's *2004 Annual Report*,[3] the CLU involved a staff of attorneys and investigators whose dedicated function is "to act as the point of contact for criminal law enforcement agencies whose work would be enhanced through cooperation with the FTC on consumer fraud issues."[4] Unlike the somewhat opportunistic criminal referrals of the past, the CLU was charged with the task of proactively identifying appropriate and interested law enforcement agencies for specific types of fraud cases, as well as educating criminal enforcement authorities about the FTC's mission and expertise. According to the annual reports, the CLU triggered thirty-eight criminal prosecutions in the year ending March 2005, in addition to six "Scofflaw" prosecutions. The numbers increased to 130 defendants being referred for criminal prosecution in the year ending March 2007.

While past performance is no guarantee of future results, there is every reason to believe that the current trend of CLU effectiveness will continue. The FTC defense bar no longer can be complacent about the criminal exposure of their clients. Indictments and convictions may not happen in the vast majority of cases, but it would be difficult in 2007 to assert that the risk of criminal liability is not "foreseeable" in much of the FTC's work.

Lessons for the FTC Practitioner

The increasing criminalization of consumer protection enforcement has brought corresponding and significant challenges to the private practices of lawyers engaged in consumer protection defense. One growing concern is the increased risk of failing to advise a client about the need to protect against possible criminal enforcement. Another is the greater risks surrounding getting retained and getting paid.

Defending the Quasi-Criminal Matter. Gone for the foreseeable future are the days when FTC counsel could look at a new Section 13(b) matter and assume virtually no risk of criminal exposure. Knowledge of the nuances of FTC law still is an important asset for counsel, but often the main questions are less whether a successful defense can be mounted or a favorable settlement reached and more whether the defendant will get to keep any of his assets and avoid criminal prosecution.

At what point should FTC counsel raise the possibility, however remote, of criminal liability? On the plus side, doing it early certainly focuses the client's attention. On the other hand, it is rarely welcome news and may cause a skeptical client to be more wary of counsel's other advice than might be warranted.

As a practical matter, it may not be wise to wait very long. Whether the risk is substantial or not, the client should have a chance to make an informed choice while it is still a meaningful decision, before any personal documents or deposition testimony are provided. When admissions could be critical to a criminal charge, "taking Five" too late might be like not taking it at all.

Who should advise the client about Fifth Amendment rights and risks of prosecution generally? Should counsel depend on themselves and their partners or refer the client to an independent firm with criminal expertise? As with the timing issue, there are multiple considerations here. On the one hand, the client who does not want to hear about potential criminal liability is also unlikely to relish the advice to hire a separate criminal defense lawyer in addition to FTC counsel. And where an asset freeze is in place (discussed below), it may be difficult enough to engage one lawyer, much less two. The decision is complicated by the fact that cases with asset freezes are the very ones for which the need for good criminal counsel may be most urgent.

The decision to assert a Fifth Amendment privilege, either as to documents or testimony or both, usually will be a de facto decision to throw in the towel in the FTC matter. Because assertion of a Fifth Amendment privilege can be used in evidence in a civil case and even used as a basis for a finder of fact to draw adverse inferences, it is unlikely that a defendant can assert the privilege and still defeat an FTC case that is based on an "unfair or deceptive" standard. Therefore, the decision to assert the privilege requires a careful balancing of factors.

When a firm has both FTC and criminal expertise, there is no sound reason why a client should not receive both FTC and criminal advice from the same firm. Where the chances of a criminal prosecution are really remote (although technically possible), it should be enough for FTC counsel to advise of the remote risk and let the client make the expected decision to defend. But where the risk of a criminal case is more than remote or the client expresses real concern about the consequences of a criminal case, one must be sure that one firm can provide good and objective advice on both fronts. This is especially true given the consequences of a decision to assert a Fifth Amendment privilege. At that point, the nature of the civil defense so changes that it will be important for the criminal defense expert to take the primary lead in the defense, letting FTC counsel (from the same or another firm) play a supportive, consulting role as needed.

Are there professional risks in failing to advise about the Fifth Amendment privilege? We have found no clear authority that holds an attorney in an FTC action liable for malpractice for failure to warn of the risks of a criminal proceeding. At the same time, an informal survey (very anecdotal) of FTC and other defense counsel revealed a nearly unanimous view that there well could be some risk in letting a client incriminate himself without appreciating the consequences.

There is case law that an attorney who claims to be an expert in a particular field, such as bankruptcy, will be held to a higher standard of expertise in that field. Logic suggests that the same higher standard could apply when a lawyer claims special expertise in the law and procedure of the FTC or another agency. One can fairly ask, given the FTC's history in the last ten years, whether "expertise in FTC enforcement" would comprise expertise in considering the risks of criminal prosecution, just as it might include expertise in the risks of parallel state or private class actions.[5]

The FTC is not a federal agency that can pursue parallel civil and criminal tracks. When agencies like the IRS or the SEC conduct civil investigations while hiding the fact that the evidence gathered may be used for a parallel, but undisclosed, criminal investigation, a court may even dismiss an indictment.[6] There have been many cases, of course, where the FTC may be pursuing a Section 13(b) case while simultaneously conferring with criminal authorities. Does the FTC have an obligation to disclose the criminal investigation in those circumstances? We have found no authority that holds that it does; nor have we found cases where the issue was raised as a defense.

The FTC in recent consent agreements includes the recital that this "action and the relief awarded herein are in addition to, and not in lieu of, any other civil or criminal remedies that may be provided by law." Does that provide adequate "notice" of criminal risk to a defendant? It certainly does provoke questions from uneasy clients. Counsel must explain that it is standard boilerplate, but should add that there are "no guarantees" that there will not be a criminal prosecution. One can certainly add (if it is true) that there has been no indication of any such action.

In any event, it is hard to imagine that such a notice would be adequate, if a notice were required in the first place. First, it is "pro forma," which courts have distinguished from the kind of actual notice that would be required if a party is a target of a pending parallel criminal investigation. Second, it does not surface, if at all, until the parties are on the verge of settlement—long after any required notification of any pending criminal proceedings would be useful to a defendant.

In the absence of a specific warning from the FTC, the need for a "criminal case" warning to a client will not always be obvious. If an investigation is initiated with a CID, the full scope of alleged wrongdoing may not be apparent to FTC counsel at the very outset. It is somewhat easier, of course, when the matter begins with an ex parte TRO and asset freeze, because the FTC's papers typically lay out much of the "incriminating" evidence. In these cases, however, counsel may have only several days to prepare for a preliminary injunction hearing and even some of that time may be needed for expedited discovery by the FTC. There simply may not be enough time to make a considered judgment about criminal exposure and asserting Fifth Amendment rights. In fact, as noted below, it can be challenging enough for the attorney to be in a position to enter an appearance and participate in the litigation in such a short time.

In some cases, the nature of the conduct alleged by the FTC itself should alert FTC counsel to the possibility of a criminal charge. In other cases, the risk may turn on facts not yet known to the lawyer and, for that reason, overlooked in assessing criminal risk.

In November 2001, for example, the FTC announced that a New York publishing company and individuals had agreed to pay $30 million to settle a Section 13(b) complaint about unauthorized credit card charges stemming from use of an adult Web site. It was not until more than two years later that some of the FTC parties and others were indicted and pled guilty in the Eastern District of New York to charges based on the same conduct. According to some published reports,[7] the criminal case resulted from wiretaps in New York in which John Gotti was caught talking about his association and work with one of the defendants. An FTC staff attorney who worked on the case was quoted as acknowledging "the [FTC] never uncovered any link between [the company] and organized crime." Apparently, the U.S. Attorney in Brooklyn had found ample evidence.

Consider the perspective of FTC defense counsel. The matter appeared on the surface to be a deceptive advertising case where the adequacy of online disclosures could be debated one way or the other. One would not be confident that a client would confide during an FTC civil inquiry, even if he knew, that "there may be some wiretap evidence of John Gotti talking about me or my codefendant." An extreme case? Perhaps, but one that shows how difficult it can be for FTC counsel to weigh the real criminal prosecution risks in a timely manner.

Getting Engaged and Paid. Even in the "good old days" before the escalation of criminal enforcement, getting paid in Section 13(b) cases was not a "lock." First, if the client made an initial retainer payment, but refused to make subsequent payments, the law firm could be "stuck" under many local court rules unless the district judge granted a motion to withdraw, a decision that is often conditioned on the substitution of new counsel. There are certainly examples where the refusal of a trial judge to allow counsel to withdraw without substitute counsel converts the matter into an involuntary "pro bono" case.

Even clients who are well-intentioned on meeting their financial obligations may find themselves in bankruptcy in the course of Section 13(b) litigation. In the absence of a security interest, law firms typically are unsecured creditors in these situations and run a serious risk of not being paid, particularly if the litigation results in a substantial judgment.

Add to these normal risks the existence of an asset freeze, often ordered on an ex parte basis before the defendant is served with the complaint. Ex parte TROs and asset freeze applications were utilized in the early 1990s, but considered by most Commissioners to be extraordinary relief under the Federal Rules of Civil Procedure that were to be used quite sparingly and only in the most clear-cut fraud cases. The standard clearly has shifted over fifteen years so that an asset freeze has become the FTC's weapon of choice in consumer fraud litigation. The FTC rarely proffers evidence that the named defendant is likely to dissipate assets. Rather, the argument more typically is that some other defendants have dissipated assets in the past and one cannot be sure it will not happen in this case as well.

Historically, the Commission's argument has been that the freezing of assets is required to ensure funds for consumer redress or other monetary relief. Increasingly the Commission's agenda has been less to preserve redress funds and more to stop a defendant in its tracks without funds to pay operating expenses or mount any defense. In one 2007 case, defendants were required to represent themselves pro se in a factually complex case, having been denied access to any funds even for living expenses, much less to hire an attorney. The Court even denied access to funds for consultation with a criminal law expert about the need to assert a Fifth Amendment privilege.[8] In the same case, a court-appointed receiver has sought payment of close to $1,000,000 from frozen funds.

In another pending case, a district judge denied separate FTC requests for a TRO and a preliminary injunction that would have limited individual defendants to a total of $1,000 for business and living expenses and attorney's fees for the federal court action.[9] In these and other similar instances, it is increasingly apparent that the real objective of an asset freeze application is less to preserve funds for redress, and more to achieve total victory without litigation, even where there may be good defenses to some or all of the FTC's claims.

The mere possibility of an asset freeze, ex parte or otherwise, adds to defense counsel's burden of getting paid or even deciding to appear in a case. Counsel have little or no control over their situation when a court hears a noticed motion for an assert freeze. Defense counsel must file an appearance to participate in the hearing but, unless the court allows for a "limited appearance" for purposes of the asset freeze or preliminary injunction hearing (hardly a safe gamble), counsel runs the risk of having appeared in the case and

then having an order limiting or prohibiting the payment of attorney's fees while not being allowed to withdraw.

One solution that seems workable at first is to consult with the pro se defendant, without entering an appearance, until it becomes clearer whether funds will be allowed for legal defense. The approach may seem reasonable, but it is hardly a clear cut solution. The local rules in some federal districts appear to place a blanket prohibition on assisting pro se applicants without filing an appearance.

Even when an asset freeze is drafted or modified to allow reasonable defense costs, substantial legal and ethical hurdles can remain for counsel. Most asset freezes are not absolute, but provide that certain "clean" funds can be used for any purpose. For example, a defendant typically cannot "incur debt," by loan, credit card, or otherwise. However, the defendant normally can accept a "gift" from a spouse, other relative, or a friend. Asset freezes also do not apply, as a rule, to "new" money earned by the defendant after the entry of the order and arising from conduct that does not violate the TRO or preliminary injunction, as the case may be. Such a structure gives some leeway to the defendant, but still leaves uncertainty for counsel.

For example, it can be quite difficult to ascertain that fees tendered consist of clean money under the order. How can counsel assure that money tendered was a "gift" to the defendant rather than a loan or the incurring of a debt? One good practice in such situations is to accept the funds directly from the spouse or other third party, rather than from the defendant. One may also take the further step of obtaining from the donor a written confirmation that the funds are being treated as a gift and that there is no undisclosed condition or present expectation of being repaid by the defendant.[10]

Determining whether fees constitute "new" money earned in compliance with the order and law generally is no small task. On the one hand, defense counsel may be forced to take the defendant's word for the source of the money. On the other hand, even when money clearly was earned after entry of a preliminary injunction, the FTC staff may argue that the money resulted from advertising or practices that were not modified sufficiently to comply with the preliminary injunction. In any of these events, any comfort that the fees were paid in accordance with the asset freeze may have to be based on a best efforts approach by counsel. Such care should avoid risk that counsel will be held in contempt for violation of the court's order, but does not guarantee that counsel will be able to retain fees that, even without his knowledge, may not satisfy the order.

Conclusion

We live in a regulatory world where nearly half of the annual complaints to the FTC involve identity theft and more than two-thirds involve the Internet in one way or another. On their face, it can be difficult to determine whether some of the complaints involve large companies, two guys in a garage, or a band of international terrorists. The odds are great that, for many of these kinds of cases, new offenders will emerge as quickly as existing ones are silenced. The trend towards criminalization of consumer protection likely will progress rather than abate.

The new electronic world has changed the roles of both the FTC and defense counsel. Many of the FTC's statutory tools, like CIDs and Special Reports, may have little effect when they must be used to deal with conduct that could be characterized as criminal under existing federal law. The FTC is turning more and more to making criminal referrals and providing assistance to prosecutors, as it should. One can hope that, in time, the FTC will have adequate resources to carry out its traditional mission of maintaining fair competition for mainstream companies and consumers alike.

The same shift has put new and different burdens on FTC defense counsel. A thorough knowledge of FTC law and civil litigation experience—administrative or federal court—may no longer be enough to protect the new style of FTC defendant. Sensitivity to criminal prosecution risks and knowing how to deal with them may be necessary to protect clients fully. And they may also be necessary to protect the lawyers themselves from professional and financial risks. ■

[1] Federal Trade Comm'n,The FTC in 2007: A Champion for Consumers and Competition (2007), *available at* http://www.ftc.gov/opa/2007/04/annualrpt.shtm

[2] FTC v. U.S. Oil & Gas, FTC File No. 812 3232. Press Release, Fed. Trade Comm'n, Victims of Oil and Gas Lease Scam to Get Back Nearly Full Refund Following $47 Million Settlements of FTC and Related Cases (Apr. 30, 1991), http://www.ftc.gov/opa/predawn/F93/usoil&gas7.txt.

[3] Federal Trade Comm'n, Fulfilling the Original Vision: The FTC at 90 (2004).

[4] *Id.* at 19.

[5] FTC defense lawyers on the competition side might face these same questions during investigations under Section 1 of the Sherman Act, 15 U.S.C. § 1.

[6] *See generally* United States v. Stringer, 408 F. Supp. 2d, 1083 (D. Or. 2006).

[7] *See* MSNBC, *Alleged Mobsters Guilty in Vast Web, Phone Fraud*, http://www.msnbc.msn.com/id/6928292/page/3/.

[8] FTC v. Int'l Product Design, Inc., Case No. 1:97-cv-01114-AVB (E.D. Va. 1997) (Motion for Contempt filed Jan. 8, 2007).

[9] FTC v. Rawlins & Rivera, Inc., Case No. 6:07-cv-146-ORL-18KRS (M.D. Fla. Jan. 31, 2007).

[10] One loose end, not yet resolved to the author's knowledge, is whether the defendant can agree to repay the gift if, after a final judgment in the case, the defendant has unfrozen funds available. There is no clear policy reason why such a repayment should not be allowed under those circumstances. The logical extension of that question, of course, is whether the donor can have a "conditional" expectation of being repaid only if, in fact, the defendant is in a position to do so when the case is finally resolved and no asset freeze restrictions remain. Whether such an arrangement would be viewed as a sensible result or a sham avoidance of the order may depend on the particular facts (e.g., spouse versus friend) but, in any case, it may be difficult for counsel to determine the actual situation at the point of need.