Avoiding Online Identity Theft and Representing its Victims

by Richard L. Ravin

Identity theft is the fastest growing crime in America, according to the United States Postal Inspection Service, and in 2006 alone, cost nearly 10 million American victims a total of five billion dollars.[1] A Federal Trade Commission (FTC) survey estimated that in 2005, eight million people in the U.S. were victimized, representing a 25 percent increase in the number of victims as reported by the postal inspector.[2] The FTC estimates that losses from identity theft totaled at least $15 billion for 2006.[3]

Ninety percent of all identity theft involving wrongful use of, or access to, existing accounts (as distinguished from fraudulent creation of new accounts) relates to credit cards, checking accounts, telephone service, and Internet payment accounts (*e.g.* PayPal).[4] Although neither the postal inspector nor the FTC quantify the fraudulent procurement of identities via the Internet, by extrapolating the data reported by the two agencies, it is clear that a substantial amount of identity theft occurs online.[5]

Online Threats to Privacy of Personal Information

Wi-Fi Hotspots

Among the newest concerns for online theft of personal information is the proliferation of Wi-Fi hotspots. As these public networks have become ubiquitous, they have also become fertile ground for electronic eavesdroppers and spoofers to capture personally identifiable and confidential information.

Unencrypted Wi-Fi networks provided at hotels, airports, cafés, libraries, or other public places, are not protected by federal and state wiretap or electronic eavesdropping laws. Unencrypted transmissions between the user's computer and the Wi-Fi access point are susceptible to being lawfully intercepted (perceived) by other nearby computer users running 'sniffer' software. Using such Wi-Fi hotspots substantially increases the risk of unauthorized disclosures of personal information such as user names, passwords, account numbers, credit card numbers, Social Security numbers, and other confidential information, such as trade secrets and attorney-client privileged communications.[6]

For attorneys, the use of Wi-Fi hotspots poses significant risk, as sending or receiving unencrypted or non-password-protected confidential information could lead to a breach of an attorney's ethical obligation to protect client confidences pursuant to Rule of Professional Conduct 1.6. Unlike communications protected by the wiretap laws (*e.g.*, the part of an email transmission that occurs via wire, common carrier, or utilizing encryption), transmissions carried over Wi-Fi hotspot networks without encryption or access controls arguably are not entitled to a reasonable expectation of privacy, and are, therefore, not a reasonable means of transmitting client confidences.[7]

Phishing Scams

Phishing remains a formidable online danger. Phishers will assume the identity of a trusted or legitimate entity, and then ask the victim to divulge personal identifiable information. The term 'phisher' applies to a cyber con artist who casts a wide 'fishing net' in the form of spam, in the hopes of catch-

ing a small percentage of victims.

In a typical phishing scam, an email directs the recipient to visit a website where he or she is urged to update personal information due to some fictitious problem. The recipient is asked to provide information such as a user name, password, credit card account number, bank account number, or Social Security number that the legitimate organization would already have. These bogus websites have the look and feel of the authentic website, and are designed exclusively for the purpose of stealing the personally identifiable information of its victims. In order to pull off the scam, the phisher uses the trademarks of legitimate organizations to fool victims. Phishing is also known as brand or trademark spoofing.

Phishers often make the links in their emails appear to be pointing to a legitimate URL (web address), but the actual URL (appearing in the web browser address bar after clicking on the link) may in fact be slightly different than the legitimate URL, such as www.msnbilling.com in a phishing scam against MSN, or www.paypalsys.com in a spoof against PayPal. Apart from the use of email, phishers can also cast their phishing nets via viruses and worms, which create pop-up ads asking for personal data.

Pop-up Windows and Framing

To mask the real URL, phishers and spoofers sometimes use pop-up technology. This is done by showing the genuine website in the main browser window and then showing the phisher's website in a window that pops up on top of it. This causes the address bar of the genuine website to appear in the background, even though the user may be inputting information into the pop-up window, thus allowing the phishers and spoofers to collect the information.[8]

Framing technology is also used by spoofers to cause the content of one website to be displayed within another. Spoofers can manipulate the display of the browser address bar so that it appears as if the first website (the spoofer's) is seamlessly part of the second's (*e.g.*, a legitimate bank's).[9] In such situations, the spoofer could cause the browser address bar to display https (the 's' stands for secure) and a locked padlock icon, signifying secure socket layer protocol, even though the information being transmitted is being fraudulently captured. As a practical matter, it is always safest to type the known authentic URL directly in the browser address bar rather than clicking on links in emails.

Sub-Domains Masquerading as Second-Level Domains

Another method used to trick email recipients is using third-, fourth- and fifth-level sub-domains in the web address of the link. For example, in one actual phishing scam, emails were sent to look as though they were from Amazon.com, with the forged message having a link that appeared to be the legitimate Amazon.com domain name. The URL (web address) became visible when mousing-over the hyperlink "To confirm your identity with us click here," which revealed the following URL: https://secure.amazon.com.execacc-ro.com/signin.php?exec/[remainder of lengthy URL omitted]. Although "Amazon.com" appeared in the URL, the part of the address—"execacc-ro.com"—that appeared later in the string (to the right), was the controlling domain.

The top-level domain (TLD) is ".com," and each label (separated by a period) to the left of the TLD specifies a subdivision or sub-domain of the domain. Thus, "execacc-ro" is the second-level domain, and it is this portion of the URL that is registered through the Internet Corporation for Assigned Names and Numbers (ICANN) domain name registration system.[10]

Sub-domains lower than the second level are created and controlled entirely by the website host. Because sub-domains are not registered, they arguably are not covered by the ICANN uniform dispute resolution policy, or by those aspects of the federal anti-cyber-squatting Consumer Protection Act (Section 43(d) of the Lanham Act) that require registration of the domain name.[11]

Keyloggers

Compounding the phishing problem are phishing-based programs called trojans and keyloggers. Such programs are designed for the purpose of collecting information from the end-users in order to steal those users' credentials. Unlike most forms of keyloggers, those used for phishing have tracking features that attempt to look for specific activities, such as capturing login names and passwords for financial institution, online retailers and e-commerce merchants, and then send them to the attackers.[12]

Federal Laws

Phishing and Spoofing Run A-Foul of Federal Laws

Phishing and spoofing often violate the Lanham Act prohibitions, including false designation of origin at Section 43(a), infringement of a registered mark at Section 32(1), and anti-cybersquatting at Section 43(d),[13] or equivalent state law unfair competition claims. Other causes of action may also be implicated, including the Computer Fraud and Abuse Act (CFAA)[14] and the CAN-SPAM Act.[15] The CFAA, however, requires jumping through hoops when used in this context, as its focus is on the unauthorized access to a 'protected computer,' not obtaining and using personally identifiable financial information. A 'protected computer' is one used in interstate or foreign commerce or communication, such as a computer connected to the Internet.[16]

The CAN-SPAM Act, while prohibiting false and misleading use of email header information (in the "from" field,[17] for

instance), limits the right of private civil enforcement to "Internet access service" providers.[18] Otherwise, enforcement is left to a multitude of federal and state agencies and authorities, such as the Federal Trade Commission, which have the right to bring civil and criminal actions against violators.[19]

Depending on the facts and circumstances involved, other claims, such as copyright infringement, may be applicable if content is copied and is otherwise protectable under copyright law. Contributory or vicarious copyright liability against the web-hosting entity may also be available. The Gramm Leach Bliley Act (GLBA) would apply to any 'pretexting' (the practice of obtaining personal financial information through false pretenses).[20] Various other causes of action may apply, including common law fraud, state consumer fraud or unfair business practices laws, and in certain circumstances, perhaps trespass to chattels. Finally, identity theft is a federal crime.[21]

No Federal Private Right of Action

It should be noted that neither the GLBA, with respect to "personally identifiable financial information" maintained by banks, securities firms, and insurance companies, nor the Health Insurance Portability and Accountability Act (HIPAA), with respect to "individually identifiable health information" maintained by healthcare providers, permit any private right of action against such organizations for unauthorized or wrongful disclosure of personal information under these statutes.[22]

Fair Credit Report Act

As discussed below, the Fair Credit Reporting Act (FCRA)[23] gives consumers access to their credit reports and allows them to limit access to their reports by third parties under certain circumstances. Although the FCRA does allow for civil liability for failing to comply with the act,[24] it does not provide for a private right of action against companies whose databases are the source of the personal information that was unlawfully obtained by third parties as a result of a security breach or phishing attacks.

State Laws

New Jersey's Identity Theft Prevention Act, Unfair Competition Law and Criminal Code

New Jersey's Identity Theft Prevention Act,[25] which became effective in 2006, has five key provisions: 1) a consumer may place a credit (or security) freeze on his or her credit report,[26] 2) a creditor shall not deny credit to, or reduce the credit limit of, an individual solely because that individual was a victim of identity theft,[27] 3) companies have a duty to notify their New Jersey resident customers whose personal information has been the subject of a security breach, or whose records are reasonably believed to have been accessed by an unauthorized person,[28] 4) businesses and public entities are required to thoroughly destroy customer records no longer being retained,[29] and 5) businesses are restricted regarding the use and display of Social Security numbers.[30]

Additionally, New Jersey's unfair competition laws may be applicable in connection with the misuse of a company's mark,[31] and New Jersey's Criminal Code makes it a crime to impersonate another to obtain a benefit by fraud.[32]

Plan of Action to Stop Further Identity Theft and Repair Credit Damage

In the event that one confirms the wrongful use of his or her identity, the victim must work with the banks and businesses where the unauthorized transactions occurred and the bogus accounts were opened to establish that he or she is not legally responsible for the subject accounts and transactions. The checklist accompanying this article and the laws and remedies discussed below provide: 1) assistance in the repairing of credit and prevention of further credit damage or property loss of confirmed victims, and 2) steps that can be taken by those who merely suspect that their identities have been stolen.

Free Credit Reports

The FCRA gives every consumer the right to receive one free credit report from each of the three nationwide consumer reporting companies every 12 months.[33] Reports can be requested online. The FRCA also provides a process for consumers to dispute accuracy of their credit reports.[34]

Initial and Extended Fraud Alerts

The FCRA provides that consumer credit reporting bureaus must grant two types of free fraud alerts when requested by a consumer: initial and extended. An initial fraud alert is granted when a person suspects that he or she has, or is about to be, a victim of identity theft. The initial fraud alert lasts for 90 days, and can be renewed if appropriate. To implement the alert, the consumer can contact the three national consumer reporting companies.[35] An extended fraud alert requires the victim to provide a copy of a law enforcement agency report (such as a report filed with the police or FTC) to one of the three national credit reporting companies.

When an initial fraud alert is placed on a credit report, it entitles the consumer to order one free credit report from each of the consumer reporting companies. Consumers may request that only the last four digits of their Social Security number appear on these reports.[36] If the consumer has already been victimized, an extended fraud alert can be requested, which lasts for seven years. When an extended fraud alert is placed on a credit reporting record, then "potential creditors" must contact the consumer before credit can be extended in his or her name, and the consumer is

entitled to two free credit reports from each of the consumer reporting companies within 12 months. In addition, if requested, the consumer reporting companies must remove the victim's name from marketing lists for pre-screened offers of credit for five years.[37]

Credit Freeze

The most restrictive precaution is a credit freeze (or security freeze), which allows the consumer to restrict access to the credit report and prevent potential creditors and certain other people and businesses from accessing the consumer's credit report. The availability of a credit freeze depends on state law or a consumer reporting company's policies. Some states charge a fee for placing or removing a freeze, although placing or removing a fraud alert is free. Placement of a credit freeze does not affect the consumer's credit score, or prevent the consumer from obtaining free annual credit reports, opening a new account, applying for a job, renting an apartment, or buying insurance.[38]

Pursuant to the New Jersey Identity Theft Prevention Act,[39] New Jersey consumers have the right to place a security freeze on their credit reports. For a New Jersey resident, the procedure for placing a credit freeze for each of the three national credit reporting agencies can be found at www.state.nj.us/lps/ca/brief/securityfreeze.pdf, and is free of charge.[40] According to the act, when a person requests a credit freeze, the credit reporting agency must: 1) within five business days, comply with the request, 2) send written confirmation of the freeze at the consumer's request, and 3) include a personal identification number (PIN) or password when sending the written confirmation to the consumer.[41] Under New Jersey law, a creditor is not permitted to deny credit to, or reduce the credit limit of, an individual solely because that individual was a victim of identity theft.[42]

FTC Complaints and Identity Theft Affidavits

Complaints of identity theft can be filed with the FTC directly online (www.ftc.gov), via the FTC's toll free Identity Theft Hotline at 877-ID-THEFT (438-4338), or in writing to the FTC. Filing an FTC complaint allows law enforcement to use the information as part of their investigation, and may help prevent further injury to a consumer's credit, accounts, or assets. To learn about filing an FTC ID theft complaint, go to www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html. To access and fill out an online complaint form, go to: https://www.ftccomplaintassistant.gov/.

An FTC identity theft affidavit form should be filled out and provided to

Checklist for Representing Identity Theft Victims

Once it is suspected or confirmed that one's identity has been 'stolen,' the following is a checklist of what to do:

1. Notify affected banks and businesses (*e.g.*, banks that issued credit cards or where affected bank accounts are located). Change PIN numbers and passwords.
2. Order a free credit report from each of the three national credit-reporting companies, pursuant to the Fair Credit Reporting Act (FCRA) (www.annualcreditreport.com/cra/index.jsp).
3. Place an initial fraud alert on credit reports.
4. File a complaint with the FTC (fraudulent use or misuse of Social Security numbers is reported to the FTC, not the Social Security Administration).
5. File complaints with law enforcement, such as the U.S. postal inspector, (http://postalinspectors.uspis.gov/forms/IDTheft.aspx), state attorney general, and/or local police (where property or account is located).
6. Place an extended fraud alert on credit reports.
7. Place a freeze on credit reports as permitted by state law (not federal). For New Jersey, *see* New Jersey's Identity Theft Prevention Act, N.J.S.A. 56:8-161 through 56:8-166.
8. Notify the state division of motor vehicles if driver's license information is suspected of being used.
9. Prepare an FTC identity theft affidavit, which is used to obtain records from banks and businesses, but is not filed with the FTC (www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf).
10. Obtain records (such as credit applications and account statements) from banks and businesses that have opened accounts or extended credit in the victim's name without the victim's authorization to help establish that the victim is not legally responsible for subject transactions or accounts. Banks and businesses may require an FTC identity theft affidavit and/or law enforcement criminal reports before releasing records.
11. Keep a record of the names and phone numbers of people with whom the victim discussed the case, and of all reports and supporting documents.
12. Make claims on applicable insurance policies, including homeowners for identity theft coverage, if applicable.
13. Dispute accuracy of credit reports using the FCRA dispute process (www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm).

banks and businesses to obtain records of accounts opened in the victim's name, or concerning transactions in the name of the victim. [43] This form does not get filed with the FTC.

The FTC is also the official agency for reporting the misuse or fraudulent use of one's Social Security number. [44]

U.S. Postal Inspection Service

In addition to investigating mail fraud, the U.S. Postal Inspection Service is a leading federal law enforcement agency in the investigation of identity takeovers. The responsibility of the postal inspectors includes protecting postal customers from fraud schemes and other crimes that may occur online and involve the misuse of the mail or of the U.S. Postal Service. This includes the use or sale of stolen or counterfeit access devices, such as credit card numbers; 'protected computers' (*e.g.*, computers connected to the Internet) without proper authority or exceeding authorized access; using computer communications in a scheme to defraud; using a false identity when sending commercial emails to mislead or deceive recipients, as with spam; and unauthorized access to communications that are stored electronically via a communications service. [45]

Insurance

Victims should check applicable insurance policies, such as homeowners, business, errors and omissions, etc. Some policies expressly cover the costs of restoring one's identity or credit (as distinguished from the loss of property) caused by identity theft, including attorneys' fees. Note, however, that some business policies may have a false pretense exclusion, which can nullify provisions that might otherwise cover the loss due to theft of identity.[46]

Conclusion

As the crime of identity theft continues to outpace all other U.S. crimes, lawyers need to be aware of their own use of the Internet and be prepared to counsel their clients, some of whom will inevitably fall victim to the crime. As a first line of defense, federal and New Jersey laws allow victims to receive free copies of their credit reports, as well as prevent access to those reports by third parties. Thereafter, the victims and their attorneys must begin the process of invalidating fraudulent transactions and closing bogus new accounts that were opened at financial institutions and businesses, by dealing directly with these entities.

Spotting fraudulent account activity quickly, by monitoring one's own accounts and credit reports for unauthorized transactions, is an important step to avoid pervasive credit damage or property loss. Victims who receive notice or otherwise suspect that their identities have been the subject of a security breach must act quickly. ⚖

Endnotes

1. http://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx, accessed on July 1, 2008; Identity Theft brochure, Safeguard Your Information, Publication 280, December 2007 at www.usps.com/cpim/ftp/pubs/pub280.pdf; accessed on July 1, 2008.
2. Federal Trade Commission – 2006 Identity Theft Survey Report, November 2007, found at www.ftc.gov/os2007/11/SynovateFinalReportIDTheft2006.pdf, accessed on June 25, 2008; FTC Finds 8 Million Identity Theft Cases, November 28, 2007 found at www.consumeraffairs.com/news04/2007/11/ftc_idtheft.html, accessed on June 25, 2008.
3. Federal Trade Commission – 2006 Identity Theft Survey Report, Nov. 2007, found at www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf , accessed on June 25, 2008.
4. *Id.*
5. *Id.* The study revealed that 56 percent of all victims of ID theft did not know how their ID information was wrongfully obtained. Although the FTC study did not separately categorize identity theft via the Internet, the FTC did report in a 2008 study that of all complaints filed with the agency for the years 1995 through 1997, about one-third represented identity theft, and of all fraud complaints filed with the FTC (excluding identity theft) about 40 to 45 percent were Internet-related for the years 2005 through 2007. "Consumer Fraud and Identity Theft Complaint Data January - December 2007" at www.ftc.gov/opa/ 2008/02/fraud.pdf, accessed on July 1, 2008.
6. Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§2511, Interception and disclosure of wire, oral, or electronic communications prohibited; 18 U.S.C. §§2510(16), ECPA Definition of "Readily accessible to the general public"; 7 N.J.S.A. 2A:156A-3, New Jersey Wiretapping and Electronic Surveillance Act (WESA), Interception, disclosure or use of wire or oral communications; violation; penalty; N.J.S.A. 2A:156A-2. Definitions, NJ WESA; New Jersey Wiretapping and Electronic Surveillance Act (WESA); *see*, Using Public Wi-Fi Hotspots Can land You in Hot Water by Risking Disclosure of Confidential Information, *New Jersey Lawyer Magazine*, Right to Privacy Issue (April 2008), Richard L Ravin.
7. *See, Id.*; New Jersey Rules of Professional Conduct, 1.6, Confidentiality Information; New Jersey Ethics Opinion. No. 701, April 24, 2006, Electronic Storage And Access of Client Files.
8. *See*, www.banksafeonline.org.uk/phishing_explained.html, accessed on July 11, 2008.
9. *See*, Royal Bank of Canada Phishing,

CyberInsecure.com, http://cyberinsecure.com/royal-bank-of-canada-phishing/, accessed on July 13, 2008.

10. To do a WHOIS database lookup, one would use the TLD and second-level domain—"execacc-ro.com", not the portions of the URL "secure.amazon.com" which are merely third-, fourth-, and fifth-level domains intended to fool the Internet user into thinking they are at the real Amazon.com website.
11. *See,* ICANN Uniform Domain Name Dispute Resolution Policy, found at www.icann.org/en/dndr/udrp/policy.htm. Accessed on Sept. 30, 2008, and 15 U.S.C. §§1125(d).
12. Anti-phishing Work Group, www.antiphishing.org/reports/apwg_report_dec_2007.pdf, accessed June 22, 2008; CNET, http://news.cnet.com/Phishing-attacks-take-a-new-twist/2100-1029_3-5695874.html?hhTest=1, accessed on July 14, 2008.
13. Lanham Act, 15 U.S.C. §§1125(a), §§1114(1), and §§1125(d).
14. Computer Fraud and Abuse Act, 18 U.S.C. §§1030.
15. CAN-SPAM Act, 15 U.S.C. §§7701 *et seq.*
16. Computer Fraud and Abuse Act, 18 U.S.C. §§1030(e)(2)(B). The CFAA also requires $5,000 in loss of use or damages regarding each "protected computer." Computer Fraud and Abuse Act, 18 U.S.C. §§1030(a)(4) and (5).
17. CAN-SPAM Act, 15 U.S.C. §§7704(a)(1).
18. CAN-SPAM Act, 15 U.S.C. §§7706(g).
19. CAN-SPAM Act, 15 U.S.C. §§7706(a) through (f).
20. Gramm Leach Bliley Act, 15 U.S.C. §§6821 through 6827.
21. 18 U.S.C. §§1028.
22. Gramm Leach Bliley Act, 15 U.S.C. §§6805; Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d-6; *see, University of Colorado Hospital v. Denver Publishing Co.* 340 F. Supp. 2d 1142 (D. Col. 2004).
23. Fair Credit Reporting Act (FCRA) 15 U.S.C. §§1681 through §§1681x, amended in 2003 by the Fair and Accurate Credit Transactions Act (FACTA), *see e.g.,* 15 U.S.C. §§1681c-1, §§1681g, and §§1681j.
24. 15 U.S.C. §§1681o.
25. N.J.S.A. 56:8-161 through 56:8-166 , and N.J.S.A. 56:11-44 through 56:11-52.
26. N.J.S.A. 56:11-46.
27. N.J.S.A. 56:11-51.
28. N.J.S.A. 56:8-163(a).
29. N.J.S.A. 56:8-162.
30. N.J.S.A. 56:8-164.
31. N.J.S.A. 56:4-1 *et seq.* and 56:3-13.16.
32. N.J.S.A. 2C:21-17. Impersonation; theft of identity; crime.
33. The requests can be staggered throughout the year for continual monitoring.
34. To Buy or Not To Buy: Identity Theft Spawns New Products and Services To Help Minimize Risk, accessed on June 29, 2008, www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.shtm; https://www.annualcreditreport.com/cra/index.jsp, accessed on July 1, 2008; Fair Credit Reporting Act (FCRA) 15 U.S.C. §§1681 through §§1681(x); *see, particularly,* 15 U.S.C. §§ 1681(c-1), §§ 1681(g), and §§ 1681(j); *see* 15 U.S.C. §§ 1681i for disputing accuracy of credit report (*see also,* www.ftc.gov/bcp/edu/pubs/consumer/credit/crez/.shtml, accessed on Sept. 29, 2008).
35. The toll free phone numbers for the three major credit bureaus are: Equifax: 1-800-525-6285; Experian: 1-888-EXPERIAN (397-3742); TransUnion: 1-800-680-7289. Any one agency that the consumer calls is required to contact the other two, resulting in the alerts being placed on the consumer's report.
36. To Buy or Not To Buy: Identity Theft Spawns New Products and Services To Help Minimize Risk, accessed on June 29, 2008, www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt05.shtm.
37. *Id.*
38. *Id.*
39. N.J.S.A. 56:11-44 to 56:11-52 and N.J.S.A. 56:8-161 to 56:8-166.
40. New Jersey's Identity Theft Prevention Act, How to Place a Security Freeze on Your Credit Report, found at the website of the New Jersey Department of Law and Public Safety, Office of the Attorney General, accessed on June 29, 2008 at www.state.nj.us/lps/ca/brief/securityfreeze.pdf.
41. N.J.S.A. 56:11-46 to 56:11-47.
42. N.J.S.A. 56:11-51.
43. An FTC Identity Theft Affidavit form with instructions can be obtained at: www.ftc.gov/bcp/eduresources/forms/affidavit.pdf; *see also* N.J.S.A. 56:11-51.
44. *See,* www.ssa.gov/oig/hotline/index.htm#idtheft, Office of Inspector General, website, accessed on July 1, 2008).
45. *See,* http://postalinspectors.uspis.gov/aboutus/laws.aspx, accessed on July 1, 2008. Identity theft reports can be filed on line with the postal inspector at http://postalinspectors.uspis.gov/forms/IDTheft.aspx.
46. *See, Lakeland Bank v. Wholesale Outlet, Inc.* 2008 WL 2445076, Appellate Division, Superior Court of New Jersey (2008), Not Reported.

Richard L. Ravin *is a member of Hartman & Winnicki, P.C., and heads the firm's Internet and intellectual property law practice areas, as well as concentrating in business law, commercial litigation, and bankruptcy law, with offices in Paramus and New York City. He is current (and founding) co-chair of the Internet and Technology Law Committee of the New York State Bar Association's Intellectual Property Law Section and past chair of the association's Intellectual Property Law Section. The author is grateful for the assistance of Shifra Apter, associate with the firm.*