Appendix D
Network Crime Resources

A. Federal Law Enforcement Contacts

Computer Crime and Intellectual Property Section (CCIPS)
Criminal Division, U.S. Department of Justice
1301 New York Avenue, N.W., Suite 600
Washington, DC 20530
Tel: 202-514-1026
Fax: 202-514-6113
http://www.cybercrime.gov
http://www.usdoj.gov

Prosecution of, and guidance, support, resources, and materials for prosecuting domestic and international network crime offenses; development of network crime policy; and support and coordination of the federal prosecution of network crimes.

Federal Bureau of Investigation
Cyber Intrusion Division
J. Edgar Hoover FBI Building
935 Pennsylvania Avenue, N.W.
Washington, DC 20535
http://www.fbi.gov
Tel: 202-324-5613
Fax: 202-324-9197

Responsible for all network crime investigations. For a list of field offices, see http://www.fbi.gov/contact/fo/fo.htm.

United States Secret Service
Criminal Investigation Division
Department of Homeland Security
950 H St., N.W.
Washington, DC 20223
202-406-9330
http://www.secretservice.gov

Investigative responsibilities include computer and telecommunications fraud, financial institution fraud, false identification documents, access device fraud, electronic funds transfers, and money laundering as it relates to these violations. For a list of field offices, see http://www.secretservice.gov/field _offices.shtml.

B. On the Web

Internet Crime Complaint Center (IC3)
1 Huntington Way
Fairmont, WV 26554
Tel: 800-251-3221; 304-363-4312; complaint center: 800-251-7581
Fax: 304-363-9065
http://www.ic3.gov

Partnership between NW3C and FBI. Allows victims to report fraud over the Internet; alerts authorities of suspected criminal or civil violations; offers law enforcement and regulatory agencies a central repository for complaints related to Internet fraud.

Cybercrime.gov

The CCIPS website, http://www.cybercrime.gov, provides information about the topics on which the Section focuses, including computer crime, intellectual property, electronic evidence, and other high-tech legal issues. The website includes news on recent criminal investigations and prosecutions in these areas, background information on cases, and speeches and testimony by Department of Justice officials. Also available on cybercrime.gov are legal research and reference materials on computer crime and intellectual property, including three manuals for prosecutors and law enforcement published by CCIPS on intellectual property, electronic evidence, and this manual.

C. Publications

U.S. Department of Justice, *Searching and Seizing Computers and Electronic Evidence in Criminal Investigations* (Office of Legal Education 2002). Provides comprehensive guidance on compute-related search issues in criminal investigations. The topics covered include the application of the Fourth Amendment to computers and the Internet, the Electronic Communications Privacy Act, workplace privacy, the law of electronic surveillance, and evidentiary issues.

U.S. Department of Justice, *Prosecuting Intellectual Property Crimes* (Office of Legal Education 2006). Presents comprehensive descriptions and analysis of all federal criminal intellectual property laws, including copyright, trademark, theft of trade secrets, counterfeit labeling, the Digital Millennium Copyright Act, and alternative mainstream criminal statutes that can be applied to intellectual property theft, including mail and wire fraud, the Computer Fraud and Abuse Act, and the interstate transportation of stolen property statutes. This manual emphasizes practical suggestions for investigating such cases, anticipating defenses, dealing with victims and witnesses, and obtaining effective sentences.

U.S. Department of Justice, *Identity Theft and Social Security Fraud* (Office of Legal Education 2004). Authored by the Fraud Section of the Criminal Division, this manual includes detailed sections on prosecutions under 18 U.S.C. §§ 1028 (identity theft), 1029 (aggravated identity theft), and 1343 (mail fraud and wire fraud).

Best Practices for Seizing Electronic Evidence (3d ed.). A pocket guide published by the U.S. Secret Service for first responders to an electronic crime scene. This document is available at http://www.forwardedge2.com/pdf/bestPractices.pdf.