



# CORPORATE HOMICIDE™

## LIFE IN A GLOBAL ECONOMY

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE

**Sentencing** - - - Adding new teeth to Federal Laws governing High-Tech crime, the U. S. Sentencing Commission sent Congress guidelines for judges that would substantially increase penalties for such crimes as credit and identity theft, using computers to solicit or sexually exploit minors and violating copyrights or trademarks online. **Most of the new standards will take effect on Nov. 1 unless Congress strikes them**, which it rarely does. **The copyright and trademark provisions take effect immediately because Congress gave the commission authority to act quickly** to stem a practice that one trade association estimated costs the software industry \$11.4 billion each year. In some cases, the new guidelines will more than double the sentence for computer and other high-tech crimes. **For example, a pedophile that used the Internet to initiate a sexual relationship with a minor** would face 41 to 51 months in prison if the case went to trial. Under current guidelines, a sentence of 18 to 24 months would be imposed, depending on other circumstances.

**Credit Card Theft Targeted** - - -The new guidelines also are expected to have a significant impact in the prosecution of credit card theft, **particularly in cases in which information on many thousands of cards is obtained over the Internet**. Calculations of the amount of loss attributable to a theft will now place a value of \$500 on the data for each card stolen, whether or not it was fraudulently used. Currently, data for such cards is valued at \$100. The change will allow prosecutors to sharply increase the amount of the loss attributable to credit card thieves, which is key in determining the sentence. **For example, a thief who stole data on 10,000 credit cards would be considered to have caused \$5 million in losses**, as opposed to \$1 million under current guidelines. That would allow a judge to impose a sentence of between 41 and 51 months if the case goes to trial, in contrast to a recommended penalty of 30 to 37 months under current guidelines.

**Copyright or Trademark Violations** - - - The commission took a similar approach in addressing violation of copyright or trademark using the Internet or other communications technologies. **The value of stolen software will be calculated based on the retail price charged by the manufacturer rather than the price the pirate put on the stolen goods**. In a case where a thief was charging \$5 for copies of a computer program that retails for \$100, for instance, the losses would be twenty-fold higher when the sentence was calculated. That would result in a sentence of from 37 to 46 months, in contrast to an 8 to 14-month range under current guidelines.

**The guidelines also call for harsher penalties for thieves who upload purloined software so that others can make illegal copies and in cases involving organized crime**. They also increase penalties by up to 25 percent for identity theft in cases where the criminal was **“breeding” documents - the practice of using stolen identity information to acquire additional forms of false identification or to commit financial fraud**. They also allow judges to impose harsher penalties in cases where the criminal assumes the victim's identity or causes substantial harm to the victim's reputation or credit rating. The recommendations were drafted at the instruction of Congress to bring federal sentencing guidelines in line with new laws intended to crack down on computer- and Internet-related crimes.

---

**Security Outsourcing Solutions, Inc.®**

One Liberty Square, 6th Floor, Boston, MA 02109 • 100 Ardmore Road, Needham, MA 02494-1833

**Theft** - - - A federal grand jury has indicted 17 people for allegedly conspiring to infringe the copyright of more than 5,000 computer software programs that were available through a hidden Internet site. **“This group is one of the oldest and most sophisticated networks of software pirates anywhere in the world,”** said Scott R. Lassar, U.S. Attorney for the Northern District of Illinois. “These defendants are accused of illegally reproducing copyrighted software and distributing it over the Internet.” Twelve of those indicted allegedly were members of an underground international group known as **“Pirates with Attitudes”** that disseminates stolen software, including programs not yet commercially available, the Justice Department said. These included a Microsoft Corp. employee who allegedly supplied company programs to the group members and to the Internet site. The remaining five defendants were employees of Intel Corp., four of whom allegedly supplied computer hardware to the piracy organization in exchange for obtaining access for themselves and other Intel employees to the group’s pirated software, which had a retail value of more than \$1 billion, the statement said. The investigation was made public with the February 3 arrest of Robin Rothberg, of North Chelmsford, Massachusetts, identified as a leader of the group by the Justice Department. **“This is the most significant investigation of copyright infringement involving the use of the Internet conducted to date by the FBI,”** said Kathleen McChesney, the special agent in charge of the FBI’s Chicago Field Division. “It demonstrated the FBI’s ability to successfully investigate very sophisticated on-line criminal activity.” **Each of the 17 defendants was charged with one count of conspiracy to infringe copyrights, which carries a maximum prison term of five years upon conviction, along with a \$250,000 fine plus possible additional financial penalties.** They will be arraigned in U.S. District Court in Chicago.

**Privacy** - - - The Internet has become the information resource of the new millennium but it’s a two way street. **When we surf the Net, we leave little trails of where we’ve been, how long we were there and what we did while we were there.** This tracking is inherent in the design of the browsers and email programs we use to access the Internet. Java applets, ActiveX, cookies, email and more all leave trails. **But you can fight back and become truly anonymous on the Internet with the help of sites such as Anonymizer.com.** Anonymizer.com is a web site. There’s nothing to download, no software to run. You simply log onto Anonymizer.com, surf and send email from their location. That’s it. **All Anonymizer.com basically does is act as an information shield.** Normally, when you arrive at a web site, your browser reveals to that site where you came from and where you are going to when you decide to leave. Using Anonymizer.com prevents all of that from happening because you always arrive and leave from Anonymizer.com’s protected location. **To access a web site, for example, you simply type in the address from Anonymizer.com’s screen which takes you to that site after they strip off any identification tags that would normally be associated to you and your location.** You arrive anonymously and leave the same way. You can also save your bookmarks with the Anonymizer.com prefix to make those frequently visited sites an easier task.

**Email is handled in much the same manner.** You first go to Anonymizer.com, compose, address and send an email using their screens. Your email arrives to any location with total anonymity. None of the identification information can be seen from within the email message or on any of the routing tags. **Anonymizer.com works so well that many of its users are government and intelligence agencies according to the company’s president, Lance Cottrell.** So what happens if Anonymizer.com is subpoenaed to reveal the source of an email placed through its service? According to Cottrell, there is no information to be subpoenaed. Anonymizer.com keeps no records because, according to Cottrell, “...it’s too easy to get our courts to issue a subpoena these days.”

**Ballistics Testing** - - - The US Air Force Research Laboratory Information Directorate has awarded \$99,908 contract to Wetstone Technologies Inc. of Freeville, N.Y., to analyze cyber weapons currently in use. The one-year agreement, **“Seized Cyber-Weapon Analysis & Prediction,”** will be basic research funded by the Air Force Office of Scientific Research. Wetstone scientists and engineers will study equipment and software that have been used in criminal or other unlawful cyber activities,” said Dr. Leonard Popyack, a scientist in the directorate’s Information Grid Division. **“The key aspect of the program is to study seized equipment and analyze it.”** The U.S. Secret Service will provide seized equipment. Wetstone researchers will also collaborate with the newly established **Computer Forensics Research and Development Center at Utica College (N.Y.).** “We will be seeking to answer several questions based on the analysis of the equipment,” said Popyack. **“Researchers will attempt to determine the level of sophistication of the technology used in the illegal activities, as well as**

**Visit our Web Site!**

[www.security-outsourcing.com](http://www.security-outsourcing.com)

**the threat it poses to the Air Force, the Department of Defense, private industry and businesses, and the national infrastructure.** Additional questions to be answered include: who developed the technology and when was it originally designed, developed and manufactured; what was the sophistication of developers, designers and manufacturers; what countermeasures are currently being used by cyber criminals; and are hidden capabilities present in the seized equipment and software.

**Fraud-One Stop Shopping - - The Justice Department and FBI launch a Web site on which consumers and businesses can report suspected Internet frauds. The center will provide law enforcement at all levels—federal, state and local—with something they have been asking for a long time: a one-stop shopping approach to identifying Internet fraud schemes and referring them to the proper agency,** Reno said at a news conference. Assistant FBI director Ruben Garcia, head of the bureau's criminal investigative division, said the center would send the complaints to the appropriate federal, state, local or even foreign law enforcement agencies. **The center also will analyze complaints, compile statistics and propose strategies for dealing with people who commit crimes using computers.** "The Internet is used to commit the same types of fraud the FBI has traditionally investigated—telemarketing, money laundering, securities fraud—but traditional investigative methods are ineffective in this new environment," Garcia said. **The largest age group using the Internet, 18- to 34-year-olds, account for 39 percent of users, Garcia said. But people over age 50 are the fastest growing group of Web users and, as a group, they surf the Internet 19 percent longer than all other age groups combined.** "Those older users are on longer and have the most assets available for investment, so they are more likely to be targets for criminals," he said. **Last year, the Federal Trade Commission received nearly 18,000 complaints of Internet consumer fraud, including allegations about online auctions and sales of computer hardware and software.** The Securities and Exchange Commission gets 200 to 300 complaints a day about possible securities fraud on the Internet. **The Morgantown, W. Va.-based Internet Fraud Complaint Center** was set up in cooperation with the **National White Collar Crime Center**, a national support network funded by the Justice Department to aid state and local prosecutors, agents and regulators in dealing with high-tech economic crime.

**Credit Card Scam Update - - A New Jersey man has admitted to a scheme in which he used personal information gleaned from the Internet to set up hundreds of fake credit card accounts in the names of the nation's highest-ranking military officers. Lamar Christian, 32, of Trenton, N.J., pleaded guilty in U.S. District Court to one count of conspiracy to commit bank fraud.** Federal prosecutors say Christian created 331 fake credit accounts and used them to buy \$161,000 worth of computers and jewelry online. The cards were set up in the names of many of the nation's highest-ranking officers, including former Army Gen. John Shalikashvili, who was President Clinton's top military adviser until he retired in 1997. Another man, Nevison Stevens, 29, of Trenton, pleaded guilty in the case earlier this year. Both men face up to four years in prison when they are sentenced. Christian is to be sentenced Aug. 3. Stevens' sentencing is scheduled for June 22.

**Wiretap Warrants - - In a case with broad implications for communications technology, lawyers for the Justice Department and a coalition of telecommunications and privacy groups square off in federal court to argue whether the FBI should be allowed to intercept Internet communications and pinpoint the locations of cellular phone users without first obtaining a search warrant. At issue in the proceedings before the U.S. Court of Appeals in Washington are rules issued last year by the Federal Communication Commission spelling out how telecommunications providers will be required to comply with the Communications Assistance for Law Enforcement Act (CALEA), passed by Congress in 1994.** The act requires telecommunications equipment manufacturers and service providers to build into their systems the capability for surveillance of telephone line and cellular communications, as well as of services such as advanced paging, specialized mobile radio and satellite-based systems. **After telecommunications providers were unable to reach agreement with FBI officials on how to implement the monitoring capabilities, the FCC adopted rules that in several areas went beyond the CALEA language** - including a requirement that cellular phones be traceable and that information on any digits dialed after a call is connected, which could include such things as account or credit-card numbers or call-forwarding instructions, must be provided. **As interpreted by the FCC, the act also would require telecommunications providers to turn over "packet-mode communications" - such as those that carry Internet traffic - without the warrant required for a phone wiretap.** Taken in total, the FCC rules amount to a "significant expansion" of law enforcement's ability to monitor private communication, said Jim Dempsey, senior staff counsel for the Center for Democracy and Technology.

## LOGON TO...SOS-DueDiligence.com

**FREE** Due Diligence Investigative Price Quotes—Online—24 hours a day/7 days a week!

### JUST THE FACTS

**SAVE MONEY** - Our clients are paying 25% to 50% less for their Investigative Due Diligence services.

**REDUCED REPORT CYCLE TIMES** - On average our clients have reduced their report cycle time by 25%.

SOS-DueDiligence.com is committed to providing professional investigative services in a cost effective, efficient and timely manner. SOS-DueDiligence.com allows you to make informed business decisions regarding mergers, acquisitions, investments, litigation, fraud, or to simply establish a business relationship.

### Free Quotes • Competitive Pricing • Timely Reports

SOS-DueDiligence.com, providing business information tools for the 21st Century.

*Corporate Homicide is a newsletter published for the exchange of information, ideas, theories, and related topics, and may not be construed as legal advice. The information provided is "general information," not "specific advice." We refer you to your professional legal and/or security providers for required services or specific advice. The publisher does not necessarily endorse opinions expressed by contributors. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in the Corporate Homicide Newsletter.*

*Circulated quarterly to businesses. To receive future issues please register at [www.security-outsourcing.com](http://www.security-outsourcing.com) by completing the **Ask the Experts form**. Also specify if you would prefer to receive Corporate Homicide via e-mail. Feedback and suggestions on future topics are welcome. © 2000. Security Outsourcing Solutions, Inc.®*



SECURITY  
OUTSOURCING  
SOLUTIONS, INC.®

One Liberty Square, 6th Floor • Boston, MA 02109

May/June 2000

Ronald R. DeLia, Publisher

# CORPORATE HOMICIDE LIFE IN A GLOBAL ECONOMY™

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE