GLOBALIZATION AND THE LONG ARM OF U.S. LAW

Richard V. Wiebusch, Esq.

Stephen A. Jonas, Esq.

March 30, 2000
London

HALE AND DORR LLP

GLOBALIZATION – U.S. LAW LOOKS OUTWARD

- Expanding U.S. and European economies and international commerce
- Consolidation and mergers in telecommunications and banking
- The Internet and global e-commerce
- Reduction in violent crime and focus on regulatory and financial violations
- U.S. Congress and Administration focus on new forms of terrorism and theft of technology

U.S. LAW – THE ECONOMIC ESPIONAGE ACT

- Prohibits theft of business, scientific, technical trade secret information
- Defendants can be non-U.S. citizens
- Jurisdiction based on effect in U.S. or involvement of U.S. business
- Enacted in 1996; 19 prosecutions to date
- 800 active FBI investigations – a high Justice Department priority
- *U.S. v. Four Pillars, Py Yang and Sally Yang (1999)*: Conviction for attempting to steal trade secrets from Ohio plant. Highlighted a problem with the Act: how to prosecute for theft of trade secrets without disclosing the trade secrets in a public trial

U.S. LAW – COMPUTER FRAUD AND ABUSE ACT

- Prohibits unauthorized access to computers and use of information
- Neither computer nor defendant need be in U.S.
- U.S. victim or effect in U.S. is sufficient
- Forfeiture provision
- In light of recent Internet disruptions, more legislation expected

U.S. LAW – FOREIGN CORRUPT PRACTICES ACT

- Prohibits payments or offers to foreign government officials or political parties to obtain or retain business
- Public company record-keeping provision
- Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (U.S. sponsored in May 1997 - would require each of the world's richest countries to enact legislation similar to FCPA)
- Activities of non-U.S. company with U.S. parent or affiliate may fall within FCPA

U.S. LAW – FOREIGN CORRUPT PRACTICES ACT (Continued)

- *SEC v. Triton Energy Corp. (1997)* (Senior executives of parent company personally charged for failing to devise an adequate system of internal accounting controls to detect and prevent improper payments by employee of foreign subsidiary)
- *SEC v. Montedison S.p.A. (1996)* (Civil suit against Italian firm whose ADR's were listed on NYSE, based on failure to report bribes in Italy to Italian officials, caused by defective internal accounting controls)

U.S. LAW – SECURITIES LAWS

- Regulates purchase and sale of securities and conduct of public companies affecting the markets
- Investigation handled by FBI, SEC, IRS, Justice Department
- Jurisdiction based on effect on U.S. securities markets
- Non-U.S. activities affecting or potentially affecting markets can be reached (e.g., the failure to block a U.S. citizen's access to a foreign Website is considered evidence of an intent to have a substantial impact on the U.S. See Restatement 3d of Foreign Relations Law of the U.S., § 416)

U.S. LAW – SECURITIES LAWS (Continued)

- Recent law enforcement emphasis on Internet securities fraud
- Cases accepting jurisdiction over non-U.S. firms and individuals
    a. *Inset Systems, Inc. v. Instruction Set, Inc.*, (1996) (advertising on the Web formed the basis for personal jurisdiction over the company in a state in which the company otherwise did not conduct business on a regular basis)
    b. *SEC v. Euro Security Fund et al* (1999): Court found personal jurisdiction over foreign nationals for insider trading, where a Virgin Islands company operating in Switzerland made some of the trades through a U.S. brokerage firm in New York City

U.S. LAW – CURRENCY TRANSFERS

- Requires reporting of receipt or disbursement of $10,000 or greater in single or related transactions
- Exempts transactions entirely outside U.S.
- IRS regulations require that financial institutions have procedures in place to detect and report possible money laundering
- Money laundering statute prohibits transfer of funds or conduct of a financial transaction in aid of or to conceal underlying offense

U.S. LAW – CURRENCY TRANSFERS (Continued)

- Treasury Department has recently upgraded its Financial Crimes Enforcement Network ("FinCen"), a computer-based operation to monitor wire transfers of funds, in order to be more effective in tracking international money laundering
- Law reaches non-U.S. citizens if conduct occurs in part in U.S.

U.S. LAW – OTHER OFFENSES

- Food Drug and Cosmetic Act
  - U.S. companies with U.K. facilities and vice versa
  - U.S. sale subjects even non-U.S. facilities to regulation and audit
  - Enormous criminal fines based on sales; debarment remedy
  - Examples of Prosecutions:
    - *U.S. v. Bard*: Government charged Bard, a medical device manufacturer, with distribution of heart catheters not approved by FDA. Resulted in $61 million fine, debarment from government contracting and 18 month prison terms for several officers (including the CEO, President, and Director of Regulatory Affairs and Quality Assurance)

U.S. LAW – OTHER OFFENSES (Continued)

- Compliance Programs can be helpful in detecting activity which is regarded as illegal under U.S. law and may reduce penalties

U.S. LAW – OTHER OFFENSES

- Antitrust statutes
  - *Microsoft* case demonstrates the aggressiveness of the Department of Justice
  - *Hartford Fire Ins. Co. v. California (1993)* – antitrust prosecution may be based on a conspiracy involving non-U.S. firm which affects U.S. customers
  - The Department of Justice has stated that it expects more international antitrust enforcement involving coordination of prosecutions in the U.S. and other countries

U.S. LAW – OTHER OFFENSES (Continued)

- False Statements
  - U.S. law makes it a felony to make an untrue statement to any federal official, agent or agency, even if not under oath
- Mail and Wire Fraud
  - Use of the mail or wires, within the U.S. or across borders, for the purpose of fraud is a felony that can be prosecuted in a U.S. court

HOW DOES U.S. LAW ENFORCEMENT WORK?

- The "Two Sovereigns" Concept
  - State and federal law enforcement authorities have independent and overlapping subject matter jurisdictions
  - Any potential violation involves satisfying both sets of prosecutors

HOW DOES U.S. LAW ENFORCEMENT WORK? (Continued)

- Federal law enforcement agencies are not centrally controlled
  - The Department of Justice
  - The U.S. Attorneys
  - The Federal Bureau of Investigation
  - The Internal Revenue Service
  - The Substantive Agencies (e.g., SEC, FDA, Commerce)

HOW DOES U.S. LAW ENFORCEMENT WORK? (Continued)

- The discretion of law enforcement agencies
- The role of the Federal Grand Jury
  - Secret
  - Serves an investigative function
- A “typical” investigation

HOW DOES U.S. LAW ENFORCEMENT WORK? (Continued)

- Mutual Assistance Treaties
  - Increasing emphasis in U.S. law enforcement
  - Treaty between U.S. and UK effective Dec. 2, 1996
- The U.S. Federal Sentencing Guidelines
  - Intended to make sentencing uniform throughout federal system
  - Increase jail time for “white collar” crime
  - Companies with a functioning Compliance Program will receive lighter sentences

WORLD BUSINESS NEWSPAPER

US ★ EDITION

FINANCIAL TIMES

www.ft.com

Friday March 24 2000

Worldwide sweep for internet fraudsters

US co-ordinates action against 1,600 suspect web sites in 28 countries

By Christopher Bowe in Washington

A worldwide sweep to target fraudulent, get-rich-quick schemes on the internet has been orchestrated by the US Federal Trade Commission with the help of international agencies.

The sweep across 28 countries – believed to be the largest of its kind – highlighted more than 1,600 suspect web sites, which will be warned to stop or change their claims. They could face investigation if they are suspected of continuing fraud.

Participants in the action ranged from the UK's Office of Fair Trading to South Korea's Fair Trade Commission. However, there was no breakdown of where the 1,600 sites were located.

The "surf project", launched in February, was part of an intensified effort by federal agencies' consumer and enforcement divisions to combat the proliferation of internet-offered scams aimed at consumers.

Officials said about 21 more limited sweeps had targeted, among other practices, pyramid schemes, unrealistic investment opportunity offerings and easy-money claims.

Enlisting the help from powerful forces, including the US Postal Service and the Securities and Exchange Commission enforcement units, FTC officials said fraudulent operators should be aware that the government would monitor the web to look for them.

"If they can use this new technology to defraud consumers, we can use it to catch them," said Jodie Bernstein, FTC director of consumer protection. "We're putting get-rich-quick schemes on notice that we're monitoring the web."

The sweep information also included details about the site owner's physical location so that the agencies can better track elusive site appearances on the internet.

The agencies have beefed up their internet surveillance to combat fraud. The US post office has 1,500 inspectors trained for internet fraud and 50 special agents for online investigations, while the SEC said it had a cyber-force of 240 surveillance officials.

FTC officials said warning e-mails were on their way to the suspect promotion sites to get them to change their claims. If the sites do not alter their promotion, law enforcement agencies in all the partnership countries would pursue efforts to shut the offending sites.

"We're going to run them off the web and, where appropriate, put them in jail," said Drew Edmondson, attorney general of Oklahoma.

However, officials said a primary goal of the effort is to get the sites to stop before consumers lose money to the schemes.

Legal action could be taken against the sites by using mail fraud laws. About half of the get-rich-quick scams follow up e-mail and internet inquiries.

Given that sites can be accessed or posted on the internet from most countries, jurisdictional issues are a factor, officials said.

Any site doing business in the US is fair game, but to take legal action against a site based in another country would have to be co-ordinated with the law officers where the operator resides.

The SEC enforcement division said it had seen more than 90 cases from the 1,600 that it intended to look into.

The effort is also establishing a permanent database, collecting information such as consumer fraud site operators, physical locations and information about the origination of files on the sites. The international partners are contributing to this database.

Pyramid schemes, the subject of previous search, have already been subject to law enforcement action by the FTC. Although a figure of the amount of consumer fraud was unclear, officials said individuals lost substantial amounts through fraud.

THE HYPOTHETICAL

- Tigerbank.com – London- based Internet banking company with state-of-the-art security system
  - Solicits customers in U.S. and Europe
  - Trades on London Stock Exchange
- Megacomm – German telecommunications company based in Berlin
  - Trades on NASDAQ and Frankfurt stock exchanges
  - Wants to provide customers with secure wireless access to bank accounts
- Megacomm and Tiger enter into licensing agreement

THE HYPOTHETICAL

- Tiger's security system protects customers from tampering by hackers but is vulnerable to internal breaches of security
- U.S. customer notices unusual administrative fee on statement and reports it to state banking authorities
- Megacomm's U.S. Agent served with U.S. Department of Justice subpoenas for documents regarding banking transactions with Tiger conducted by several of its wireless customers
- Megacomm contacts Tiger

WHAT PROMPTED THE SUBPOENA?

- U.S. customers noticed the unusual fees
- Complaint made to state banking regulators
- Regulators keep track of multiple complaints against single bank
- Reason for federal law enforcement involvement
  - Number of complaints and involvement of foreign bank
  - Law enforcement emphasis on Internet and financial fraud

COULD U.S. LAW ENFORCEMENT REACH TIGER?

- Tiger's U.S. customers – the effect in the United States
- Jurisdiction via the Internet – minimum contacts
- Prior cases
  - *Quokka Sports, Inc. v. Cup International Ltd. (1999)* (Personal jurisdiction asserted over New Zealand defendants, in part because they registered a Web domain name in the U.S.)

COULD U.S. LAW ENFORCEMENT REACH TIGER? (Continued)

- *SEC v. Stewart (1999)* (Judgment by default, after notice by publication in the Wall Street Journal (European Edition) and the International Herald Tribune, over defendants last known to operate in Paris, whose conduct occurred and had impact in U.S.)
- *David Mead and Saybolt, Inc. (1999)* (President and CEO of Western Hemisphere Operations of Netherlands-based company sentenced for bribing Panamanian official; money wired from the Netherlands to Panama directly. At the time, Dutch law did not prohibit bribing foreign officials; only contact with the U.S.; defendant sent a U.S. employee to Panama to make the payment)

CONDUCTING AN INVESTIGATION

- Should Tiger conduct an investigation ?
  - Has corporation or employees violated the law?
  - Has a government agency begun an investigation?
  - Are there reporting obligations to government agencies?
  - Do directors have fiduciary obligations to shareholders to investigate?

CONDUCTING AN INVESTIGATION

- Who should conduct the investigation?
  - Protecting the privilege
  - Dealing with the government
- How the investigation is conducted
  - Collecting documents
  - Interviewing witnesses
  - Organizing to protect the privilege
  - Avoiding obstruction of justice charges

THE RESULTS OF THE INVESTIGATION

- Internal investigation by Tiger reveals:
  - Many customer accounts subjected to 0.5-1.0% increases in administrative fees
  - Excess fees transferred to unrecorded administrative accounts and from there disbursed to European and Caribbean banks by wireless telephone transactions
  - Husband and wife senior executives have accessed the administrative accounts
  - Software engineer downloaded proprietary information and ran program across customer accounts

WHAT IS TIGER'S EXPOSURE?

- Theories of corporate criminal liability
  - Vicarious criminal responsibility

    (corporation liable for actions of employee acting within the scope of his or her employment and motivated by intention to benefit the company)
  - Collective knowledge

    (a corporation's knowledge is deemed to be the sum of the knowledge of all its employees)
  - Corporate indifference or "willful blindness"

    (a corporation's criminal intent may be shown by an employee's reckless disregard or callous indifference to the law's requirements)

WHAT IS TIGER'S EXPOSURE? (Continued)

- Mail and Wire Fraud
- Money Laundering
- Computer Fraud and Abuse
- Securities Violations
- Larceny

CORPORATE COMPLIANCE PROGRAMS

- What are they?
- Their importance under the U.S. Sentencing Guidelines
- Their importance as a management tool

CORPORATE COMPLIANCE PROGRAMS

- The typical features
  - Employee code of conduct
  - Covering the applicable legal standards
  - A vehicle for hearing from employees about potential violations
  - Compliance officers and reporting to the Board of Directors
  - Education and training
  - Appropriate discipline for violators