



U.S. Department of Justice

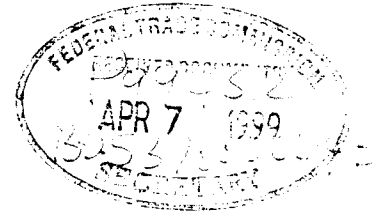
Criminal Division

Assistant Attorney General

Washington, DC 20530-0001

MAR 29 1999

Mr. Donald Clark
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Room H-172
Washington, DC 20580



Re: U.S. Perspectives on Consumer Protection
in the Global Electronic Marketplace —
Comment, P994312

Dear Mr. Clark:

The Department of Justice ("Department") hereby submits these comments in response to the notices of the Federal Trade Commission ("FTC"), filed December 15, 1998, and February 1, 1999, for comments on its Workshop on U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace ("Notice"), 63 *Fed. Reg.* 69,289 (1998), and 64 *Fed. Reg.* 5,062 (1999). The Department appreciates the opportunity to assist the FTC in its examination of these perspectives.

The following comments address five of the principal topics on which the Notice invited comments. To provide a logical structure for these comments, some of the topics have been addressed out of numerical order.

Development of the Global Electronic Marketplace

25a. What developments will hinder the growth of electronic commerce?

The growth of electronic commerce ("e-commerce") is likely to be hindered if consumers continue to have doubts about the security of personal information that they are entrusting to electronic merchants. A 1997 Ernst & Young survey of U.S. Internet shopping, for example, found that almost 70 percent of those who had not yet made a purchase on the Internet were

uncomfortable sending their credit card data over the Net.¹ Still more recently, a survey by the Pew Research center found that 61 percent of those who had never made an online purchase cited credit card security as a reason.²

Continued concerns about the security of e-commerce transactions would be undesirable at a time when, according to one recent prediction, fewer than 5 percent of e-commerce sites on the World Wide Web ("Web") will show a profit during the next 12 to 18 months.³ While many factors are likely to influence the continuing growth and direction of e-commerce, government agencies should take note of these consumer concerns in determining what it can and should do to foster that growth.

27. To what extent do/will new marketing techniques made possible by technological developments affect consumer protection?

Law enforcement agencies have observed that as more and more people acquire the capability, at work or home, to obtain access to the Internet, the Internet is becoming increasingly attractive for both legitimate and illegitimate commerce. The same components of the Internet that are used to further commercial and personal interaction, such as Web sites, E-mail, and chat rooms, are also being used for deception and defrauding of individuals and businesses throughout the United States. Some of the more prominent types of online fraud now being reported include investment schemes (e.g., securities market manipulation, or "pump and dump," schemes), online auctions involving sales of computer equipment and services or collectibles, and prize or sweepstakes-based schemes.

Certain factors -- the global nature and operation of the Internet, as well as the configuration and relative inaccessibility of information relating to the true identity and location of those who purport to offer e-commerce opportunities online -- can make it more difficult for consumers or law enforcement agencies to determine the legitimacy of an online business or to take effective action if that business fails to

¹ See Alan Stewart, "The key to building trust in e-commerce," FINANCIAL TIMES, Dec. 30, 1998
<wysiwig://212/http://www.ft.com/hippocampus/qf62ee.htm>.

² See Pew Research Center for The People & The Press, "The Internet News Audience Goes Ordinary," <http://www.people-press.org/tech98sum.htm (printed Jan. 14, 1999).>

³ See Nancy Weil, "Research Firm Sees Little Online profit in Next Year," INDUSTRY STANDARD, Jan. 5, 1999
<http://www.thestandard.net/articles/article_print/0,1454,3054,00.html>.

deliver promised goods or services or provides goods or services far lower in value than what consumers were promised. The Department notes that in a joint report to the President and the Prime Minister of Canada in November, 1997, representatives of both the United States and Canadian governments observed similar problems in the context of cross-border telemarketing fraud.⁴ In addition, some crimes that stem from systems or personal deception in e-commerce (e.g., identity theft and resulting fraudulent transactions) are likely to become more prevalent because of the global character of the Web.

28. To what extent do/will technological developments enable consumers to protect themselves?

Certain technological developments that enable individual consumers to control third-party access to personal information that they must provide in legitimate e-commerce transactions will significantly assist consumers in protecting themselves. Biometrics and properly safeguarded passwords, for example, can help to ensure that unauthorized persons cannot access individual consumers' computers. Various hardware and software solutions, such as encryption protocols, can also provide substantial security for consumers who access particular Web sites.

These technological solutions, however, assist consumers only in reducing the risk of what might be termed systems deception. Systems deception refers generally to techniques, such as data harvesting and intrusion techniques, that are intended to evade computer security measures rather than to direct false or deceptive information at human beings. Such techniques, if used by fraudulent schemes, would be employed to obtain valuable personal data, especially access devices such as credit card numbers, without the knowledge or consent of the consumer to whom those numbers are assigned. In general, personal deception - that is, the presentation of deceptive or fraudulent information to consumers, in conjunction with various influence techniques to secure their trust - is far less amenable to technological remedies. Indeed, in certain circumstances, criminals could combine techniques of systems deception, such as the use of "frame-spoofing"⁵ or "Trojan horses,"⁶ with personal deception to carry out fraudulent or deceptive practices in e-commerce.

⁴ See UNITED STATES-CANADA WORKING GROUP ON TELEMARKETING FRAUD, REPORT (1997).

⁵ See Paul Festa, "Communicator subject to frame-spoofing," CNET, Jan. 5, 1999 <<http://www.news.com/News/Item/Textonly/o,25,30558,00.html>>.

⁶ See Bob Sullivan "Trojan maps drive, lifts addresses," MSNBC, Jan. 13, 1999 <<http://www.msnbc.com/news/2318001.asp>>.

International Requirements

12. What are the minimum protections that should be available to consumers in the global electronic marketplace?

At a minimum, in any global e-commerce transaction, a consumer should be given a level of protection equivalent to what he or she is entitled to receive in offline transactions, or at least a notice about the fact that legal protections to which they are accustomed in domestic law are or may be inapplicable or unavailable in that transaction. This principle stems from the notion that consumers come to rely on domestic legal and market-based protections in the United States in conducting their affairs, and need to be aware that in e-commerce transactions with entities in other countries, U.S. legal protections may not be available and foreign law may not offer comparable protections. Implementing this principle would help ensure that consumers are not victimized by reliance on false or fraudulent premises when they deal on the Internet.

In the long term, if e-commerce is to become truly global in character, consumers should be able to expect that regardless of where they reside and where an online business is organized, has its principal place of business, or initiates its online communications with prospective consumers, they will have comparable levels of timely and effective responses to their complaints or disputes, whether those responses take the form of dispute resolution processes or government action on their behalf. This will be especially important, as consumers in one country cannot reasonably be expected to travel personally to other countries, or to retain legal counsel in those countries, to dispute particular transactions or to contact law enforcement authorities if the transactions appear to be fraudulent or otherwise criminal. Effective consumer protection in a global environment must involve developing or enhancing measures that foster legitimate e-commerce (e.g., commercial practices and dispute resolution mechanisms), as well as measures that halt or discourage illegitimate e-commerce.

Law Enforcement Agencies

14. What is the proper role for law enforcement agencies in providing effective protection for consumers engaged in global electronic commerce?

To combat fraud and deception in global e-commerce, federal law enforcement agencies, criminal, civil, and regulatory, should work together and coordinate their use of all available weapons - including criminal sanctions, civil penalties, and forfeiture - to provide strong, consistent, and credible enforcement mechanisms for consumers. While market forces and self-regulatory mechanisms can do much to shape the development of e-commerce, the Department's extensive experience in investigating and prosecuting fraud strongly suggests that market solutions

alone will not suffice to control or halt the use of fraudulent and deceptive practices on the Internet.

Government efforts to combat fraud in e-commerce should encompass national-level coordination with the FTC and other agencies, as well as more locally oriented task forces or specialized enforcement units. These approaches have worked well in coordinating enforcement resources to combat other forms of fraud, such as telemarketing fraud, securities fraud, and health care fraud. At the federal level, the Department chairs the interagency Telemarketing and Internet Fraud Working Group, which brings together federal law enforcement and regulatory agencies for regular coordination and communication on enforcement and prevention issues relating to Internet fraud. The Department also has an ad hoc Electronic Commerce Working Group, which facilitates coordination among Departmental components on various issues affecting e-commerce.⁷ In addition, the participation of the Department of Justice and the FTC in the Vice-President's interagency electronic commerce working group will ensure that law enforcement agencies can appropriately address issues relating to Internet fraud in policy discussions of policies relating to e-commerce.

This coordination and collaboration should also extend beyond federal agencies to include state and local law enforcement agencies, such as state attorneys general, that have the resources and interest to participate in coordinated consumer protection efforts. These state and local law enforcement agencies, and representative organizations such as the National Association of Attorneys General (NAAG), the National District Attorneys Association (NDAA), and the North American Securities Administrators Association (NASAA), can initiate and coordinate activities on training, investigative, and prosecutive matters relating to consumer protection and fraud in e-commerce. That coordination and collaboration should also extend to effective prevention and education measures for consumers and business, as explained further in the response to questions 19-20 below.

If the United States is to be successful in addressing fraud in global e-commerce, of course, it must do so by seeking cooperative solutions with other countries. To do so, it should first identify the most significant issues through processes like

⁷ In the preparation of these comments, for example, the Electronic Commerce Working Group was instrumental in coordinating the Department's consideration of the FTC notices and ensuring participation in the drafting process by components such as the Office of the Associate Attorney General, the Antitrust Division, the Civil Division's Office of Consumer Litigation and Office of Commercial Litigation, and the Criminal Division's Fraud Section, Computer Crime and Intellectual Property Section, and Office of International Affairs. These comments reflect the substantial contributions of these components.

this comment period and the FTC's planned workshop, and then engage other countries on these issues.

One approach would be to begin with small groups of similarly-minded countries, and ultimately expand the outreach to a larger group of nations. Starting with a smaller group of countries has been useful in other areas — including, for example, computer crime — because these countries often have a similar balance of law enforcement, privacy, and commercial concerns as the United States, making it easier to reach consensus and develop initial solutions. Thereafter, the initial countries may broaden their outreach by discussing these issues and solutions to a larger group. While the larger group is likely to have different balances of concerns from the initial group, the preliminary solutions can be a core around which a greater consensus may crystallize. Specifically, in e-commerce, the United States may want to seek out a small number of countries that have a high percentage of their populations connected to the Internet, and whose cultures are beginning to adopt e-commerce as one of the standard means of doing business, then expand the outreach to countries that are still in the earliest stages of connecting to the Internet.

When selecting the nations to approach in this area, the United States should also consider the particular groups within the nations to approach. Because the electronic marketplace is growing so quickly, driven in large measure by industry and consumer demand, a strategy for including industry in the solutions should be developed. While it is likely that the initial international contact would occur on a government-to-government basis, strong consideration should be given to including industry representatives as early as possible so that solutions developed will have been done with careful consideration to market forces and consumer demands.

The Department of Justice has had success with a similarly-structured approach in the related area of computer crime. Like international fraud, the problem of international computer crime implicates a range of issues involving national sovereignty, privacy rights, and protection of citizens, and presents significant problems. By approaching smaller groups of countries through organizations such as the G8 Group of Nations, the Council of Europe, and the Organization for Economic Cooperation and Development (OECD), the United States was able to find significant areas of broad agreement. Thus, in December 1997, the G8 Ministers met and agreed upon ten principles and ten action items in the high-tech crime area, copies of which are enclosed as Appendix A to these comments. Indeed, several of the principles — particularly those dealing with expedited preservation and sharing of data — are directly applicable to the problem of combating consumer fraud in the electronic marketplace. The Department is prepared to work in close coordination with the FTC to build upon these foundations when formulating a strategy to combat transnational fraud, and to work

with the FTC to introduce issues relating to fraud in the electronic marketplace in these and other fora.⁹

While the Department of Justice has made significant progress in the international area, more work needs to be done. For example, the Department has found that there are significant cultural and legal differences between the United States and other nations relating to disclosure of data, particularly involving the sharing of information about online consumer transactions. Because successful criminal prosecution of transnational fraud is likely to involve the expeditious sharing of such information, there is a need for further development, in multilateral fora, of mechanisms that protect the legitimate privacy interests of individual citizens of various countries but that allow critical information to be shared among law enforcement agencies.

Similarly, governments must take note of the problems raised by anonymous or pseudonymous communications over the Internet. While nations must be cautious not to create undue interference with the natural development of free and open e-commerce, they must also recognize that anonymity and pseudonymity in transactions may make consumer protection and criminal prosecution difficult or impossible, and encourage the market to develop solutions that satisfy the needs of both governments and consumers.

Finally, while an international approach may be structured to start small and grow outward, the problem should be addressed with an eye toward maximum inclusiveness. Just as banking havens are a problem in the money laundering field and data havens are a problem in the computer crime area, governments should seek to minimize the further development of fraud havens. Because the Internet makes international boundaries invisible, the existence of countries that tolerate or foster fraud within their borders could undermine even the most carefully-developed multinational enforcement scheme. Any approach should discourage, to the greatest possible extent, the creation of such havens, and encourage the maximum amount of information passed to consumers when they are dealing with companies located in such countries.

To address these and other matters relating to Internet fraud, the Administration in the near future will be launching a new Initiative to address the problem of Internet fraud. This Internet Fraud Initiative, which is being developed under the leadership of the Vice-President, will represent the first time that the Department has made Internet fraud a priority, and the

⁹ For further detail about the Department's international initiatives in the computer crime area, see the Computer Crime and Intellectual Property Section's Web page at <http://www.usdoj.gov/criminal/cybercrime/intl.html>.

first Initiative that the Department has developed to address Internet fraud through both criminal and civil enforcement.

15. To what extent do private actions provide effective protection for consumers engaged in electronic commerce with foreign businesses?

Except in truly extraordinary circumstances, where an individual consumer's or business's volume of particular e-commerce transactions with a business is so great that it is economically feasible and efficient for that consumer or business to undertake private civil litigation, private actions are unlikely to provide effective protection for consumers or businesses in transnational e-commerce transactions. The Department's investigative and prosecutive experience with fraudulent telemarketing schemes, which routinely operate in jurisdictions other than where their victims reside, indicates that private actions would be of little or no use in any commercial setting where the entity purporting to offer goods or services intends to deceive or defraud its victims. If that is true within the United States, which has uniform federal laws relating to fraud and deception, it will be even more true in a global environment with widely differing laws and enforcement authorities, particularly where the volume of an individual consumer's losses may be relatively small but the gross gain from many consumers' losses is substantial.

16. To what extent do existing laws, conventions, treaties, or practices with respect to the sharing of information among law enforcement agencies in different countries provide effective protection for consumers engaged in global electronic commerce? To what extent do they need to be modified?

In general, the Department believes that the United States and countries with which it has information-sharing arrangements for law enforcement should review the adequacy of those arrangements in relation to e-commerce transactions, and consider modifications to those arrangements where significant delay in preserving or transferring needed evidence for law enforcement purposes is likely to occur. That review may also need to address the sufficiency of substantive criminal and civil statutes against fraud, and other procedural statutes important to transnational law enforcement efforts (e.g., extradition), to ensure that there can be effective protection on a multilateral basis. In the case of certain intensively regulated industries, such as securities and banking, the United States will need to consider the possibility that modifications may need to be more extensive or different from modifications that would generally apply to e-commerce transactions for most goods and services.

In practice, the United States and other countries have a variety of informal mechanisms and practices that permit information-sharing in matters of mutual law enforcement

interest, to the extent permitted by domestic law. In addition, various federal agencies have executive agreements with their counterpart foreign agencies to facilitate information-sharing and cooperation. Finally, Mutual Legal Assistance Treaties ("MLATs") that the United States has negotiated with various foreign countries for use in criminal law enforcement matters, as well as the letters rogatory process, provide a formal framework for obtaining information and evidence available only through compulsory measures. All of these mechanisms and processes can assist in effective consumer protection in e-commerce. At the same time, the Department is aware that litigation and other matters in the requested country have sometimes caused substantial delay in transfer of important information needed for particular investigations. Such delay can be highly damaging, if not fatal, in the effective investigation of fraud involving the Internet because of the speed with which criminals can communicate and operate online. Furthermore, even expeditious processing of requests for information may not suffice for law enforcement needs if countries do not take into account the transience of data relating to e-commerce transactions. Data preservation issues will need to be addressed as part of the broader consideration of effective measures for consumer protection in global e-commerce.

17. To what extent do existing laws, conventions, treaties, or practices with respect to the coordination of law enforcement activities between different countries provide effective protection for consumers engaged in global electronic commerce? To what extent do they need to be modified?

In general, the United States and other countries interested in fostering e-commerce need to make use of existing informal and formal mechanisms for appropriate law enforcement coordination, and to modify or build upon those mechanisms where appropriate to foster effective coordination. In addition to bilateral discussions, both the G-8 and the Consumer Policy Committee of the Organization for Economic Cooperation and Development offer suitable venues for exploration of various aspects of consumer protection and e-commerce. The Department is not aware of any general laws or treaties that would bar it or other countries from intergovernmental coordination.

The Department also notes that to the extent any modifications of existing laws or practices may be considered to enhance intergovernmental capabilities for consumer protection in e-commerce, those modifications should make it clear that they are not intended to limit or narrow the scope of current United States law enforcement jurisdiction to prosecute international or transnational conduct that victimizes United States residents or corporations. Antitrust and fraud are but two of the areas in which law enforcement agencies in the United States will initiate enforcement actions in appropriate cases to protect its residents

or corporations from extraterritorial conduct that has direct effects on them.⁹

18. To what extent is there a need for international dispute resolution procedures or tribunals for law enforcement agencies seeking to protect consumers engaged in electronic commerce with foreign businesses?

With respect to the federal criminal and civil laws that it is responsible for enforcing, such as proscriptions of fraudulent and deceptive practices, the Department believes that there is no need for international dispute resolution procedures or tribunals to address violations of those laws and to seek to provide some measures to redress consumer concerns. If federal law enforcement agencies in the United States can timely obtain information needed for particular investigations of fraudulent e-commerce transactions that harm U.S. consumers or businesses, federal courts of general or specialized jurisdiction can provide appropriate fora where those agencies have determined that enforcement action is appropriate. In particular instances where consumers may have lost funds in e-commerce transactions but enforcement action may not be possible, governments should continue to explore other mechanisms for consumer redress or dispute resolution.

Consumer and Business Education

19. What steps have been and should be taken to educate consumers about the global electronic marketplace?
20. What steps have been and should be taken to educate business about consumer protection in the global electronic marketplace?

In answering these questions, it may be instructive to compare certain features of offline and online business environments:

(1) Information Search Costs. In an offline environment, consumers or businesspeople who want to buy from a local merchant can gather information about that business from others in the community, as well as from the trappings of the business itself, that can help them to distinguish between legitimate and dishonest merchants. By contrast, in an online environment, a business's Web page can make the business appear friendly and attractive, but does not necessarily rely on local or repeat

⁹ See, e.g., *United States v. Nippon Paper Industries Co.*, 109 F.3d 1 (1st Cir. 1997), cert. denied, 118 S. Ct. 685 (1998) (reinstating indictment of company for conspiracy by Japanese companies to fix price of thermal fax paper in North America, because offshore conspiracy had substantial and intended effects within United States).

traffic. Consumers cannot turn to neighbors or other local residents to learn about a particular online business. While many Web site operators will provide a forum for consumers to list comments or complaints, dishonest operators can choose to refrain from providing such a forum, or to delete negative comments and leave the impression that all of its customers are satisfied customers.

(2) Remedies. In an offline environment, at least in this country, merchandise that is not acceptable can be returned with relative ease, in part because of federal and state consumer protection laws that help to define consumers' rights. In global e-commerce, consumers who do not receive the items they ordered, or receive items of far lower value than they had expected, are likely to encounter substantial (if not insuperable) difficulty in receiving refunds or other redress under current consumer protection laws in many countries.

(3) Merchants' Risk of Loss. Offline merchants in a local community who alienate their customer bases will not obtain repeat customers, and will go out of business, losing their investment in the process. The global reach of the Internet, however, can encourage a dishonest businessperson, if he is interested only in maximizing short-term profits, to abandon any concern with "good will" or repeat business when millions of potential customers can be contacted with a few keystrokes. In addition, the cost of creating a superficially impressive Web site for that purpose, or abandoning that site after sufficient funds have been obtained from many victims, is extremely low, and therefore poses no real threat to the dishonest Web site operator's activities.

These differences make it necessary for federal, state, and local law enforcement agencies to coordinate and collaborate with appropriate private-sector entities in developing effective prevention and education measures for e-commerce. Because business-to-business transactions play such a dominant role in e-commerce,¹⁰ prevention and education efforts concerning e-commerce should be directed to both individuals and businesses. Moreover, those efforts should be addressed to each of the features discussed above:

(1) Information Search Costs. The government should take steps to reduce information search costs, and to increase the quantity and quality of consumer information on e-commerce, in several ways. First, it should encourage businesses to establish or join programs to establish digital certification for e-commerce merchants, such as a "seal" that a widely respected

¹⁰ See Bob Tedeschi, "Real Force in E-Commerce Is Business-to-Business Sales," N.Y. TIMES ON THE WEB, Jan. 5, 1999 <<http://www.nytimes.com/library/tech/99/01/cyber/commerce/05commerce.html>>.

business association or trade organization may issue for Web sites. The Department plans to initiate discussions with one or more of the organizations currently involved in such efforts to see whether it or other government entities can assist in these efforts.

Second, all levels of government should consider establishing Web sites for residents within their respective jurisdictions, to inform them about fraud and deceptive practices on the Internet. The Department and the FBI already have some information about Internet-related fraud on their Web sites. The Department is expanding its Web site to include more detailed information for consumers and businesses on which types of fraud are most prevalent on the Internet, and what steps consumers and businesses should take to respond to possibly fraudulent transactions on the Internet.¹¹ To enhance the utility of these Web sites, the Department intends to establish cross-links with other government and private-sector Web sites, such as the FTC's own Web site, to make them as informative as possible for consumers.

Third, the Department and other agencies plan to work with the private sector to encourage, as appropriate, technological approaches that increase the difficulties of committing fraud through the Internet (e.g., biometrics and protocols such as public key infrastructure and secure socket layer software), or that increase the ease with which law enforcement can receive and analyze information about Internet-related fraud (e.g., consolidating disparate sources of complaints and analyzing them). Even though technological solutions cannot by themselves stamp out all fraud on the Internet, they can be useful mechanisms to reduce its incidence and to foster public awareness about the need for appropriate caution in e-commerce transactions.

(2) **Remedies.** Even in purely domestic e-commerce transactions, consumers need to be informed through various means that dishonest merchants or criminals can easily mislead consumers about their true identities and locations, or the true value of the goods or services they offer, and make it more difficult for dissatisfied consumers to receive refunds or redress under domestic laws. For global e-commerce, consumers also need to receive notice in some form that domestic legal remedies may not be applicable or effective to resolve disputes with foreign-based businesses. Such notice could be provided through digital certification programs, dialogue boxes that inform consumers that they are dealing with a foreign firm, or traditional consumer education mechanisms.

¹¹ This information will be available in the near future at <<http://www.usdoj.gov/criminal/fraud>>.

(3) Merchants' Risk of Loss. Increased adoption of digital certification or "seal" programs may help to increase the risk of loss by dishonest merchants if consumers come to believe that such programs provide timely and reliable information about the legitimacy of the businesses participating in the programs. In addition, appropriate publicity for government enforcement efforts against Internet fraud -- including information indicating that dishonest businesspeople are receiving substantial penalties for engaging in fraudulent or deceptive conduct in e-commerce -- should enhance the perception that the risk of loss for dishonest business practices is substantial.

Finally, the Department intends to foster relationships between government and the private sector to develop specific prevention and education messaging for various types of fraud in e-commerce. Legitimate businesses that operate or facilitate payment for goods and services in e-commerce, such as credit-card issuers and other banking and financial institutions, would be particularly appropriate for development of these relationships. For certain types of e-commerce transactions -- especially securities and other forms of investment where the potential losses by individual investors may be substantial -- it may be that prevention efforts may need to be more intensive and more focused than for general anti-fraud prevention efforts.

Workshop

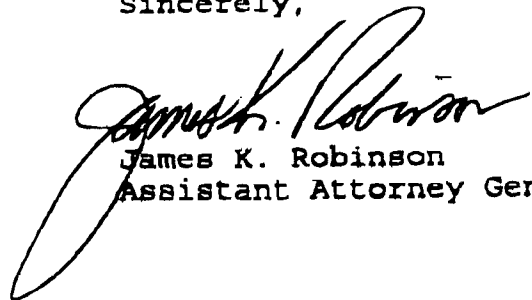
30. Which interests should be represented at the Commission's initial public workshop on "U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace?"

The workshop should be broadly representative of government and private-sector interests. Representation from the federal government should include law enforcement and regulatory agencies that conduct criminal or civil investigations or proceedings into fraudulent or deceptive practices in interstate or foreign commerce. Such agencies include the Department of Justice, the Federal Bureau of Investigation, the Postal Inspection Service, the United States Secret Service, the Securities and Exchange Commission, and the Commodity Futures Trading Commission.

Representation from the private sector should include companies that provide goods and services in or through e-commerce, including the credit card industry. The latter industry may be able to provide information of particular use to agencies that seek to combat fraud in e-commerce. That information may include an explanation of the allocation of losses in international credit card transactions, as well as suggestions for identifying possibly fraudulent entities, based on the volume of chargebacks stemming from transactions involving those entities. In addition, private-sector representation should include organizations such as BBBOnline, TRUSTe, or similar organizations involved in digital certification programs for Web sites.

The Department appreciates the opportunity to share these views with the FTC. It looks forward to continued collaboration with the FTC in developing and applying effective measures for consumer protection.

Sincerely,

A handwritten signature in black ink, appearing to read "James K. Robinson". The signature is fluid and cursive, with a large loop at the end.

James K. Robinson
Assistant Attorney General

Enclosure

APPENDIX A

Principles to Combat High-Tech Crime (from Communiqué of the G8 Ministerial on High-Tech Crime, December 10, 1997)

- I. There must be no safe havens for those who abuse information technologies.
- II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred,
- III. Law enforcement personnel must be trained and equipped to address high-tech crimes.
- IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
- VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
- IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
- X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Action Items

(from Communique of the G8 Ministerial
on High-Tech Crime, December 10, 1997)

In support of the PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.
3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.
6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.