Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

Use Our Resources
- For Law Enforcement
- For Communities
- For Researchers
- More Services

Visit Our Kids' Page

Apply for a Job

Congressional Testimony

Testimony of Thomas T. Kubic, Deputy Assistant Director, Criminal Investigative Division, FBI
Before the House Committee on the Judiciary, Subcommittee on Crime
June 12, 2001
"The FBI's Perspective on the Cyber Crime Problem"

Good morning Mr. Chairman and members of the Subcommittee on Crime. I am pleased to appear today on behalf of the Federal Bureau of Investigation and share with your Subcommittee the FBI's efforts to address cyber crime.

Let me begin by emphasizing that the FBI places a high priority on investigating cyber crime matters and is committed to working with this Subcommittee and all of Congress to ensure that law enforcement and the private sector have the necessary tools and protections to combat these crimes. It is only with the effective coordination and cooperation between all levels of government and private sector companies that efforts to combat cyber crime will succeed. The FBI recognizes and appreciates the interest and efforts of private sector companies in preventing cyber crime as well as their willingness to work with law enforcement to address the problem.

I would like to first provide an FBI perspective as to the extent of the cyber crime problem along with the unique challenges faced by law enforcement in addressing it, and then give you an overview of what the FBI is doing to address the problem including details concerning the Internet Fraud Complaint Center and a recent nationwide Internet fraud operation.

The Internet is changing the world as we know it, and promises to change how we buy things, how we communicate, where we get entertainment, news, and weather, where we work, and much, much more while bringing enormous benefits to society. The growth and utilization of the Internet as a communications and commerce tool is unsurpassed in modern history. Current trends reflect this remarkable growth:

- Internet users in the U.S. reached 65 million in 1998, over 100 million in 1999, and are expected to exceed 200 million this year. 1
- business-to-business e-commerce totaled over $100 billion in 1999 (more than doubling from 1998) and is expected to grow to over one trillion dollars by 2003. Worldwide net commerce, both business-to-business and business-to-consumer, will hit an estimated $6.8 trillion in 2004. 2

The vast majority of communication and commerce conducted via the Internet is for lawful purposes. However, the Internet is increasingly utilized to foster fraudulent schemes. Just as prior technological advances have brought dramatic improvements for society, they have also created new opportunities for wrongdoing. The unique challenges facing law enforcement in addressing cyber crime revolve around the nebulous

Top Story
Recent Stories
National Press R
Top Local News
Local News by O
Congressional Testimony
- 2006
- 2005
- 2004
- 2003
- 2002
- 2001

Major Executive
Radio
- FBI This Week
- Gotcha

Contacts
- FBI Headquar
- FBI Local Offi
- FBI Overseas

Backgrounders
- FBI Priorities
- FBI History
- Reports & Pub
- FOIA and Rea Room

nature of cyber crime. The initial stages of a cyber crime investigation involve a high degree of uncertainty. It is often difficult to quickly identify and assess what type of crime, if any, has been committed. For example, when the FBI receives a complaint indicating that a business has experienced some type of intrusion involving its computer network, the possible crimes committed are indeterminate. It could be a malicious hacking incident aimed at damaging or sabotaging the network, a possible terrorist attack, some form of espionage, a denial of service attack, as well as any myriad form or combination of traditional crimes such as frauds or extortions. Contrast this with a more traditional crime in the physical world such as a bank robbery. When a subject walks into a bank with a gun demands money, the type of crime being committed is abundantly clear to everyone. Moreover, in a bank robbery, there is typically a number of physical types of evidentiary value such as fingerprints, shoe impressions, surveillance video and/or photographs, money taken, and several witnesses. None of this is available in the commission of an on-line crime. What little evidence is available in an on-line crime will usually not exist for long. Without an immediate response by skilled cyber investigators, it will often be forever lost.

This elusive nature of cyber crime translates into a critical need for high levels of expertise in investigating cyber crime matters. It is rarely clear at the outset of an investigation as to the ultimate purpose behind a computer intrusion. However, our investigations have developed evidence that in a majority of cases, the purpose of intrusions is to facilitate ongoing criminal activity and seek financial gain.

By way of example, on March 1, 2000, a computer hacker allegedly compromised multiple e-commerce web sites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet web sites. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) police service in a search at the residence of the subject who was then arrested in the UK along with a co-conspirator under the UK's computer misuse act of 1990.

This case was predicated on the investigative work by the FBI, the Dyfed Powys police service in the United Kingdom, Internet security consultants, the Royal Canadian Mounted Police (RCMP), and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations. Loss estimates are still being determined.

As worldwide dependence on technology increases, high-tech crime is becoming an increasingly attractive source of revenue for organized crime groups, as well as an attractive option for them to make commercial and financial transactions that support criminal activity. Criminal activity in the cyber world presents a daunting challenge at all levels of law enforcement. In the past, a nation's border acted as a barrier to the development of many criminal enterprises, organizations and conspiracies. Over the past five years, the advent of the Internet as a business and communication tool has erased these borders. Cyber criminals and organizations pose significant threats to global commerce and society.

The use of the Internet for criminal purposes is one of the most critical

challenges facing the FBI and law enforcement in general. Understanding and using the Internet to combat Internet fraud is essential for law enforcement. The fraud being committed over the Internet is the same type of white collar fraud the FBI has traditionally investigated but poses additional concerns and challenges because of the new environment in which it is located. The accessibility of such an immense audience coupled with the anonymity of the subject, require a different approach. The Internet is a perfect vehicle to locate victims and provide the environment where the victims don't see or speak to the fraudsters. The Internet environment often creates a false sense of security among users leading them to check out opportunities found on the Internet less thoroughly than they might otherwise. Anyone in the privacy of their own home can create a very persuasive vehicle for fraud over the Internet. The expenses associated with the operation of a "home page" and the use of electronic mail (e-mail) are minimal. Con artists do not require the capital to send out mailers, hire people to respond to the mailers, finance and operate toll free numbers. This technology has evolved exponentially over the past few years and will continue to evolve at a tremendous rate.

Internet fraud does not have traditional boundaries as seen in the traditional schemes. No one knows the full extent of the fraud being committed on the Internet. Not all victims report fraud, and those who do, do not report it to one central repository. For traditional fraud schemes the FBI has systems in place to identify and track fraud throughout the country. For example, a con man opens up shop in Chicago, finds a location, obtains phones, hires personnel, and begins to defraud people. When victims don't receive what they were promised and realize that they have been defrauded, they will contact their local field office of the FBI, and provide the complaint information, which will be forwarded to the Chicago office (where the fraud is occurring). The FBI in Chicago receives a number of these complaints and initiates an investigation. Fraud over the Internet does not need a physical location, nor personnel, nor telephones. Internet fraud is disjointed, and spread throughout the country and other countries. The traditional methods of detecting, reporting, and investigating fraud fail in this virtual environment. Victims of fraud have been unsure of how or where to report what they see or what they have experienced on the Internet. Law enforcement agencies have received complaints in a piecemeal fashion, most not reaching a level to advance the complaint to an investigation. Another problem is venue. Without some technical investigatory steps it is difficult to identify the location of a website or the origin of an e-mail.

The Internet provides criminals with a tremendous way to locate numerous victims at minimal costs. The victims of Internet fraud never see or speak to the subjects, and often don't know where the subjects are actually located. Crimes committed using computers as a communication or storage device have different personnel and resource implications than similar offenses committed without these tools. Electronic data is perishable - easily deleted, manipulated and modified with little effort. The very nature of the Internet and the rapid pace of technological change in our society result in otherwise traditional fraud schemes becoming magnified when these tools are utilized as part of the scheme. The Internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities; the need for close coordination among law enforcement agencies; and the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases. Victims are often scattered around the country in different jurisdictions or countries than the subject(s). Subjects located in other countries are

increasingly targeting victims in the U.S. utilizing the Internet. Evidence can be stored remotely in locations not in physical proximity to either their owner or the location of criminal activity. In addition, losses suffered by victims in individual jurisdictions may not meet prosecutive thresholds even though total losses through the same scheme may be substantial. In order to subpoena records, utilize electronic surveillance, execute search warrants, seize evidence and examine it in foreign countries, the FBI must rely upon local authorities for assistance. In some cases, local police forces do not understand or cannot cope with technology. In other cases, these nations simply do not have adequate laws regarding cyber crime and are therefore limited in their ability to provide assistance. Our legal attache program provides critical contributions in these matters.

Cyber crime exists across FBI program boundaries and without regard to international borders. Among the FBI program areas impacted by cyber crime are: securities and commodities transactions, prime bank schemes, telemarketing schemes, online banking frauds, government program and private health care fraud schemes, online pharmacy schemes, online auction frauds, identity theft, intellectual property theft, business-to-business frauds, non-delivery of services, so-called Nigerian letter solicitations, credit card fraud, e-commerce and trading, e-commerce and government procurement, online gambling, organized crime/drugs, terrorism, fugitives, purchase and sale of stolen/counterfeit merchandise, child pornography, denial of service attacks, intrusions, money laundering, and as a business tool to transact criminal activity.

Criminals commonly use computers to communicate, store information, and perform financial and other transactions. Information which at one time was maintained in paper files now resides in digital format on hard drives and networks, and information that once was transmitted as analog voice over telephone connections is now transmitted in digital format over the Internet. The result is that these devices often contain critical evidence of criminal activity not only with respect to computer crimes, but also with respect to conventional crimes where use of a computer is merely incidental to the crime.

In addition to the basic investigative steps required in any investigation, cyber crime investigations require that new types of questions be asked, new clues looked for, and new rules be followed concerning the collection and preservation of evidence. In order to successfully conduct these investigations, investigators require significantly advanced skills. Regardless of whether the computer system itself is the target of criminal activity or the computer system (or Internet) is used in furtherance of a crime, the fact that a computer is involved brings into play and creates a necessity and requirement for a qualified person to competently handle the computer-related and Internet issues. Computer analysis and response team (cart) resources are heavily relied upon by field offices to respond to the wide variety of computer facilitated crimes. The FBI has supported local regional computer forensic labs (RCFL) initiatives in San Diego and Dallas. These cooperative ventures between the FBI, DEA and other federal agencies, and state and local law enforcement provide computer forensic support to all law enforcement agencies within their respective territories. The development of such regional labs is, in our view, very important, both in order to leverage law enforcement resources and to ensure the development and implementation of sound national standards for computer forensics.

To this point, we have discussed in general the potential threat posed by cyber crime, why it has become and will continue to be one of the most

significant crime problems , and briefly described some of the myriad facets of cyber crime. I would like to now focus the discussion on what the FBI is doing to address the area of cyber crime.

Internet Fraud Complaint Center (IFCC)

The development of a proactive strategy to investigate Internet fraud through the establishment of an Internet Fraud Complaint Center (IFCC) as a central repository for criminal complaints was essential. The IFCC is a joint operation with the FBI and the National White Collar Crime Center (NW3C). The NW3C is a non-profit organization which is partially funded by the department of justice. The mission of NW3C is to provide a nationwide support system for the prevention, investigation and prosecution of economic crimes. A little over a year ago, on may 8, 2000, the IFCC opened its doors to combat the growing problem of criminal fraud over the Internet. The IFCC was necessary to adequately identify, track, and prosecute new fraudulent schemes on the Internet on a national and international level. It serves as a clearinghouse for the receipt, analysis, and dissemination of criminal complaints concerning frauds perpetrated over the Internet. IFCC personnel collect, analyze, evaluate, and disseminate Internet fraud complaints to the appropriate law enforcement agency. The IFCC provides a mechanism by which the most egregious schemes are identified and addressed through a criminal investigative effort.

The IFCC provides a central analytical repository for criminal complaints regarding Internet fraud, and it acts as a resource for enforcement agencies at all levels of government to include regulatory agencies. It provides analytical support, and aids in developing and providing training modules to address Internet fraud. The FBI and the national white collar crime center (NW3C) cosponsor the IFCC . This partnership is mutually beneficial for both entities in that it allows both agencies to share staffing responsibilities and, by forwarding complaints to FBI field divisions, utilize the FBI's investigative resources to address this new techno crime.

The IFCC identifies current crime problems, and develops investigative techniques to address newly identified crime trends. The information obtained from the data collected is providing the foundation for the development of a national strategic plan to address Internet fraud.

IFCC's mission is to develop a national strategic plan to address fraud over the Internet, and to provide support to law enforcement and regulatory agencies at all levels of government for fraud that occurs over the Internet.

IFCC's purpose is the following:

- to develop a national strategy to address Internet fraud;
- to develop criminal Internet fraud cases and refer for criminal prosecutions companies and individuals responsible;
- to reduce the amount of economic loss by Internet fraud throughout the United States;
- to provide an analytical repository for Internet fraud complaints;
- to receive, analyze and refer all fraudulent activity identified on the Internet;
- to identify current crime trends over the Internet;
- to develop investigative techniques to address those identified crime problems;
- to track fraud facilitated by the Internet and provide analytical

support of Internet crime trends;
- to act as an investigative resource for Internet fraud;
- to develop training modules to investigate Internet fraud;
- to develop information packets from complaints generated and forward that information to the appropriate law enforcement agencies.

Public awareness of the existence and purpose of the IFCC is paramount to the success of this effort. The IFCC provides a convenient and easy way for the public to alert authorities of a suspected criminal activity or civil violation. Victims of Internet crime are able to go directly to the IFCC web site (www.IFCCFBI.gov) to submit their complaint information, relieving considerable frustration for the victim in trying to decide which law enforcement agency should receive the complaint. The FBI web page also aids in this effort. A detailed explanation of the complaint center, its purpose and contact numbers, is provided so that consumers can report Internet fraud. The FBI web page provides victims with a hyperlink to the IFCC web page. Many other web sites which provide information on fraud matters contain links to the IFCC web site (e.g., the Department of Justice site, www.Internetfraud.usdoj.gov).

The FBI has also established an Internet fraud council working group consisting of federal and state law enforcement agencies, international law enforcement agencies, federal and state enforcement agencies, and representatives of the private business sector. The group's purpose is to create a network to share information, discuss pertinent issues, recommend legislative solutions, and obtain the maximum benefit for all participating members.

During the start-up phase of IFCC, the entire staff processed incoming complaints and forwarded them to law enforcement agencies. In its first year of operation, the IFCC received 36,410 complaints, of those complaints, 5,907 were invalid, incomplete or duplicative, resulting in 30,503 valid criminal complaints. Those complaints were referred to an average of two to three law enforcement agencies. This referral process has spawned hundreds of criminal investigations throughout the country. The FBI staff at the IFCC have begun to use the data to identify multiple victims, various crime trends and same subject cases thus initiating the investigative phase of the center's operations. This process wasn't fully functional until January 1, 2001. Utilizing this process in which the IFCC staff draft Internet investigative reports and forwards those reports to multiple law enforcement agencies, the IFCC has investigated and referred 545 investigative reports encompassing over 3,000 complaints to 51 of 56 FBI field divisions and 1,507 local and state law enforcement agencies. IFCC has also referred 41 cases encompassing over 200 complaints to international law enforcement agencies. The IFCC has received complaints of victims from 89 different countries.

Auction fraud is by far the most reported Internet fraud, comprising nearly two-thirds of all complaints. Payment for merchandise that was never delivered accounts for 22% of complaints, and credit and debit card fraud makeup almost 5% of complaints. Another 5% of complaints stem from various types of investment frauds and confidence fraud schemes such as home improvement scams and multi-level marketing schemes. It has been the experience of the FBI that further investigation into these complaints often reveals a variety of frauds being perpetrated by subjects. Subjects engaged in one type of fraud scheme such as on-line auction fraud are frequently involved in other types of fraud schemes such as bank fraud, investment frauds and/or ponzi/pyramid schemes.

Businesses that conduct a significant amount of commerce over the Internet are exposed to losses in the millions of dollars due to various fraud schemes. With assistance from the private sector, the IFCC is developing a business- friendly system for rapid data transfer of multiple complaints in an effort to better serve these crime victim-companies' needs. This process will permit the Internet companies that are experiencing these losses to file bulk complaints and those complaints will then be distributed by IFCC to the appropriate law enforcement agencies.

In effect, the IFCC operates as part of a cyber community watch in which the self policing efforts of honest and vigilant Internet users and Internet service providers result in potential fraudulent activity over the Internet being brought to the attention of law enforcement through the IFCC. The IFCC does much more than just collect complaint information. It ensures that the information, along with additional investigative information developed by IFCC personnel, is disseminated to the appropriate agencies, and that identified fraud schemes can be prevented or mitigated. While other agencies have fraud databases that complement that of the IFCC, only the IFCC proactively provides such information to appropriate law enforcement agencies. The IFCC processes all complaints it receives regardless of the alleged dollar loss. Many of the complaints received do not allege losses which meet minimum dollar thresholds for federal prosecution, but they can often be successfully worked by local law enforcement agencies. At a minimum, they form part of a database which enables IFCC to potentially connect them with a widespread fraud scheme and/or organized criminal group. In this light, all complaints alleging fraud over the Internet are important. No victim should feel like any loss they suffered is too insignificant to report. It is only by victims and businesses reporting potentially fraudulent activity that law enforcement becomes aware of it and can take action. This point is made clear by action taken recently by the FBI and other law enforcement agencies in operation cyber loss.

The success of the IFCC was demonstrated through IFCC's key role in Operation Cyber Loss. The FBI and the Department of Justice announced on May 23, 2001 a nationwide investigation into Internet fraud, code named "Operation Cyber Loss," initiated by the FBI's Internet fraud complaint center (IFCC) and coordinated by FBI offices, U.S. Postal Inspection Service (USPIS), Internal Revenue Service-Criminal Investigative Division, U.S. Customs Service, United States Secret Service, and numerous state and local law enforcement entities. The Internet fraud schemes exposed as part of this investigation represent over 56,000 victims nationwide who suffered cumulative losses in excess of $117 million. Among the Internet fraud schemes highlighted by Operation Cyber Loss were those involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, identity theft, various investment and securities frauds, multi-level marketing and ponzi/pyramid schemes. Approximately 90 subjects have been charged as a result of operation cyber loss for wire fraud, mail fraud, conspiracy to commit fraud, money laundering, bank fraud, and intellectual property rights (software piracy). Twenty-six different FBI field offices throughout the country have been involved in the cyber loss investigation. As is true of Internet fraud in general, subjects and victims involved in this operation were scattered throughout the world. Action taken in connection with this operation represents only a small fraction of cases referred by the IFCC and only represent cases culminating in significant prosecutive action.

The schemes identified as part of Operation Cyber Loss vary widely in type and complexity. They tend to be multi-jurisdictional with subjects and

victims scattered across the United States and the world. While many of the schemes involved an element of on-line auction fraud, this was often only one aspect of a subject's fraudulent activities. The cases reflect the nature of fraudsters to migrate from one fraudulent scheme to another, and is indicative of criminal behavior that would only continue to expand if left unaddressed.

The FBI recognizes that the IFCC and initiatives such as Operation Cyber Loss, while important first steps in addressing Internet fraud, represent merely the tip of the iceberg when it comes to the threat posed by cyber crime. They are a piece of a developing comprehensive FBI strategic plan addressing all aspects of cyber crime which will allow the FBI and law enforcement to effectively and efficiently maintain a high level response capability and prosecutorial success in areas where either: (1) a computer system and/or the Internet are used in furtherance of a crime; or (2) a computer system is the victim of a crime. The use of a computer system or the Internet in furtherance of crime is not limited to one FBI program area but is increasingly found in criminal investigative division and national infrastructure protection center cases. In many instances where a computer system is seriously targeted, the purpose of the attack is to facilitate ongoing criminal activity.

The FBI has taken a number of other steps to address cyber crime. The National Infrastructure Protection Center (NIPC) was created in February, 1998, and was given a national critical infrastructure protection mission per Presidential Decision Directive (PDD) 63. The NIPC mission includes: detecting, assessing, warning of and investigating significant threats and incidents concerning our critical infrastructures. It is an interagency center physically located within the Counterterrorism Division at FBI headquarters. In conjunction with the center, the FBI created the National Infrastructure Protection and Computer Intrusion Program (NIPCIP) as an investigative program within the Counterterrorism Division. The FBI has 56 field offices with NIPCIP squads with 16 regional NIPCIP squads, which are comprised of specially trained investigators and analysts. Initial investigations into computer intrusion matters have been primarily conducted by NIPCIP squads. During the course of such investigations, it is increasingly found that the intrusion was merely the first step in a more traditional criminal scheme involving fraud or other financial gain. At this point in an investigation, the case would normally be turned over to the substantive squad handling those types of criminal schemes. This has been the case in numerous incidents involving computer intrusions into the databases of credit card companies, financial institutions, on-line businesses, etc. to obtain credit card or other identification information for individuals. This information is then used in schemes to defraud individuals and/or businesses. Due to the nature of cyber crime and the manner in which it crosses traditional program boundaries, a number of FBI field offices have formed "hybrid" squads which combine NIPCIP, cart, white collar crime, violent crime, and organized crime/drug trafficking resources and investigators on one squad to address cyber crime matters. In addition, the FBI continues to develop and operate cyber crime task forces consisting of investigators and resources from other federal agencies as well as state and local agencies. The FBI considers such task forces an efficient and effective means to leverage resources and expertise in coordinating investigations into cyber crime. The complex nature of cyber crime investigations make cooperation and coordination among law enforcement agencies vital in this area. Cyber crime task forces provide an invaluable mechanism to cover investigative areas that cross jurisdictional and program lines. The FBI plans to aggressively pursue development of such task forces in all FBI field divisions.

No less important than cooperation among other law enforcement agencies in combating cyber crime is the need for cooperation and coordination between law enforcement and the private sector. The FBI continues to place a high priority on improving and developing private sector outreach programs to facilitate reporting and investigation of cyber crime. Focus groups have been and will continue to be established with the private sector to develop long term working relationships which will aid in identifying cyber crime problems and the impact they have on their businesses as well as the formation of proactive strategies to address the threats. These relationships promote private sector reporting of criminal activity, threat assessment/warning to the private sector and private sector assistance to law enforcement (subject matter expertise, technical expertise, etc.).

Fundamental to the effectiveness of efforts to address cyber crime are identification and implementation of recruitment and training needs. Intensive training programs are necessary to support investigative efforts at the federal, state and local levels. Cyber investigators require cyber skills in the basic performance of their job. The FBI currently provides significant blocks of computer and Internet training to all its new agent classes. In addition, similar and more advanced training is increasingly provided to agents as part of standard on-going training programs.

The FBI is cognizant of all the difficulties faced by congress in contemplating any proposed legislation which would affect the Internet. It requires a delicate balancing of individual rights and potential harm to society; of free commerce and threats to national and global commerce. On-line child pornography and the sexual exploitation of children present such issues. While there are some who believe the FBI's innocent images initiative which utilizes undercover agents posing as children on-line to identify and investigate potential sexual predators to infringe upon individual rights, most would agree that this is outweighed by the potential harm to children and society in general if these sexual predators are not stopped. The FBI fully supports the department of justice's view that any legislation affecting the Internet should: 1) treat physical activity and "cyber" activity in the same way; 2) be technology neutral; and 3) be carefully crafted to accomplish the legislation's objectives without stifling the growth of the Internet or chilling its use as a communications medium.

The FBI is committed to ensuring the safety and security of those who use the Internet while maintaining an appreciation of the Internet as an important medium for commerce and communication. Focused law enforcement efforts will promote greater consumer confidence and trust in the Internet as a safe and secure medium of commerce and communication. The IFCC serves as an example of an innovative approach to an emerging crime problem. It provides the benefits of community policing, forging an effective partnership between law enforcement at all levels, ordinary citizens, consumer protection organizations such as the NW3C, and the business community. Addressing the emerging and dynamic threat of cyber crime requires contributions from all segments of our society. The FBI's IFCC serves to facilitate and coordinate this collaborative effort. Thank you.

---

1 *New York Times*, November 12, 1999
2 Source: Forrester Research, Inc., <http://www.Forrester.com>