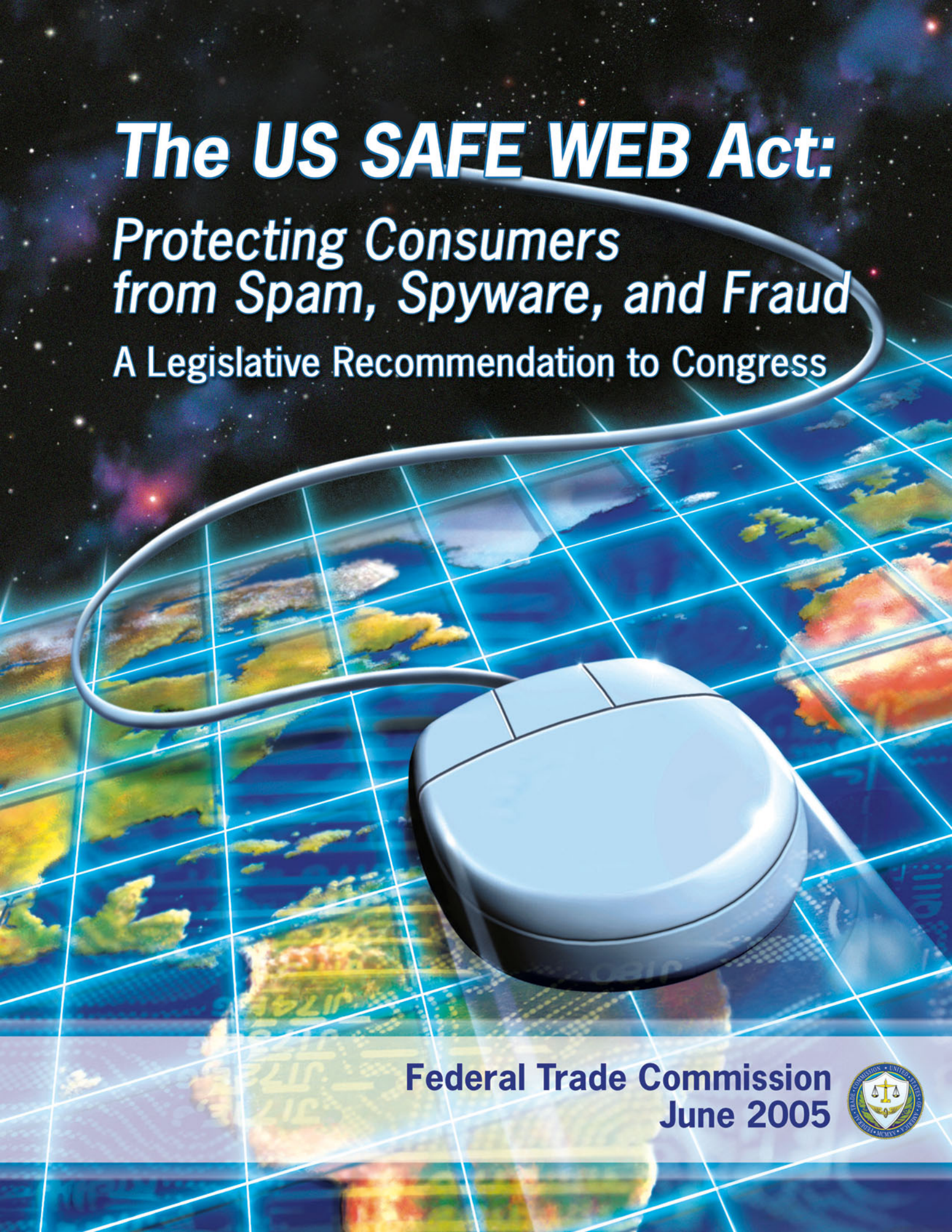
The US SAFE WEB Act:

Protecting Consumers from Spam, Spyware, and Fraud

A Legislative Recommendation to Congress



Federal Trade Commission
June 2005

The US SAFE WEB Act:

Protecting Consumers from Spam, Spyware, and Fraud

A Legislative Recommendation to Congress

June 2005

Federal Trade Commission

Deborah Platt Majoras, Chairman
Orson Swindle, Commissioner
Thomas B. Leary, Commissioner
Pamela Jones Harbour, Commissioner
Jon Leibowitz, Commissioner

Table of Contents

Executive Summary

You're sitting at your home computer to buy that dream vacation you've been saving for. You have to navigate through dozens of pop-up ads while you're surfing, and your connection is much slower than usual. You finally find the vacation deal you want, and you type in your bank account information to pay for the trip. But there's a glitch. So you call customer service and complete the transaction by phone. Meanwhile, you receive an email from your bank asking you to update your account information. You respond by sending the relevant information, including your Social Security number.

The next day, you discover your bank account is wiped out. You have no idea how this happened. After doing some research, you learn that you could be a victim of "keystroke loggers" in Eastern Europe, "phishers" in Canada, a rogue call center employee in the Philippines, or just a plain, old-fashioned fraudulent business that could be located anywhere in the world.

Today, American consumers fall victim to foreign con artists in ways unknown just a few years ago. To address this problem, the Federal Trade Commission (the "FTC" or "Commission") recommends legislation to Congress entitled the "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders Act of 2005" (the "US SAFE WEB Act").

Using Internet and long-distance telephone technology, unscrupulous businesses can strike quickly on a global scale, victimize thousands of consumers, and disappear nearly without a trace – along with their ill-gotten gains. For example, deceptive spammers can easily hide their identities, forge the electronic path of their email messages, and send messages from anywhere in the world to anyone in the world. Fraudulent overseas telemarketers can also victimize American consumers and hide their ill-gotten gains in offshore bank accounts.

In 2004, 16 percent of the fraud complaints collected in *Consumer Sentinel* involved foreign businesses or consumers. (*Consumer Sentinel* is a database of fraud and identity theft complaints maintained by the FTC.) Seventy-seven percent of these cross-border complaints were from U.S. consumers complaining about foreign businesses.

Remarkably, these high numbers understate the problem. In many more instances, consumers do not know that their complaints are against foreign entities. A "phishing" email can be sent from across the street or across the world. A call center employee who deceptively obtains a consumer's PIN can be sitting in Gary, Indiana or Gurgaon, India. A consumer might mail a check for an advance-fee loan offer to a post office box in Buffalo, New York, that is, in fact, just a mail drop for a telemarketing boiler room in Canada. Even when a U.S.-based business defrauds a U.S. consumer, the business often uses a foreign third party, such as an

Internet Service Provider ("ISP"), domain registrar, or bank, to shield information and assets from U.S. law enforcers. Indeed, discussions at FTC workshops on spam and spyware, as well as recent Congressional hearings on spyware and identity theft, highlight the international nature of these problems and show a strong need for new tools to combat cross-border schemes harming consumers.

The proposed US SAFE WEB Act would help to address the challenges posed by globalization of fraudulent, deceptive, and unfair practices. The proposed legislation largely tracks S. 1234 and H.R. 3143 from the 108th Congress, the International Consumer Protection Act.

The US SAFE WEB Act draws on established models for international cooperation pioneered by agencies such as the Securities and Exchange Commission ("SEC") and the Commodities Futures Trading Commission ("CFTC"). The FTC faces significant challenges in battling sophisticated cross-border schemes. Just as improved authority to act in cross-border cases gave the SEC and CFTC important new tools to fulfill their missions, enactment of the US SAFE WEB Act would help the FTC fulfill its mission of protecting and assisting U.S. consumers. Although not a panacea for addressing all of the challenges posed by international investigations and litigation, the US SAFE WEB Act will substantially improve the FTC's ability to meet them.

The US SAFE WEB Act would provide the FTC with new tools in four main areas.

1. The US SAFE WEB Act strengthens the FTC's ability to cooperate with its foreign counterparts.

The FTC is currently not authorized to share confidential information obtained in consumer protection investigations with its foreign law enforcement counterparts. This can hurt U.S. consumers. For example, even if both the FTC and a Canadian consumer protection agency are investigating the same Canadian telemarketer defrauding U.S. consumers, the FTC often cannot share information it obtains pursuant to its main investigatory tool, the Civil Investigative Demand ("CID"). This is true even when a Canadian action against that Canadian telemarketer would benefit U.S. consumers.

Similarly, the FTC cannot issue CIDs on behalf of foreign law enforcement agencies, even if providing such assistance would help U.S. consumers. For example, suppose a foreign agency is investigating a foreign spammer that is sending illegal spam to U.S. and foreign consumers, and a former employee of that spammer is based in the United States. If the foreign agency asks the FTC to obtain testimony for it from the U.S.-based former employee, the FTC cannot do so.

The US SAFE WEB Act would overcome existing restraints on the FTC's ability to share information and provide investigative assistance to foreign counterparts in appropriate cases, when consistent with the public interest of the United States. And, significantly, such a provision would encourage those agencies to provide reciprocal assistance in FTC cases.

2. The US SAFE WEB Act improves the FTC's ability to gather information about schemes harming U.S. consumers.

Key to successfully combating cross-border fraud and deception is the ability to take action without prematurely tipping off investigative targets. Once notified of FTC action, targets can disappear and move assets offshore, beyond the effective reach of U.S. courts. The Commission seeks to improve its ability to obtain more information from third parties without a premature tip-off to its investigative targets.

For example, many third parties, including ISPs from whom the FTC requests information in spam and spyware investigations, have stated that they will provide notice to the investigative target before they will share information with the FTC, even when no federal law requires such notice and even when they would not provide such notice in a criminal investigation. Faced with the dilemma of losing the information or losing the target and its assets, the Commission often does not send the CID. This eliminates potentially important sources of information in FTC investigations, particularly in spam and spyware investigations. The US SAFE WEB Act would allow the FTC to seek court orders requiring third parties to keep CIDs confidential for a limited period of time in appropriate cases, which would improve the FTC's ability to gather information about pernicious schemes harming U.S. consumers. The criteria for seeking such court orders under the US SAFE WEB Act is modeled on an existing provision in securities law.

3. The US SAFE WEB Act improves the FTC's ability to obtain consumer redress in cross-border cases.

The US SAFE WEB Act confirms the Commission's ability to take action in cross-border cases, including the authority to provide restitution to U.S. and foreign consumers injured by cross-border consumer protection law violations. By confirming the availability of remedies, Congress can protect Americans from foreign wrongdoers and prevent the United States from becoming a haven for wrongdoers targeting victims abroad.

Moreover, the Commission increasingly faces significant obstacles in recovering money for consumer fraud victims from foreign defendants who have foreign assets and domestic defendants who have transferred their assets abroad. The US SAFE WEB Act would allow the

FTC to target more resources toward foreign litigation to facilitate recovery of offshore assets to redress U.S. consumers.

4. The US SAFE WEB Act strengthens the FTC's participation in international enforcement projects and networks.

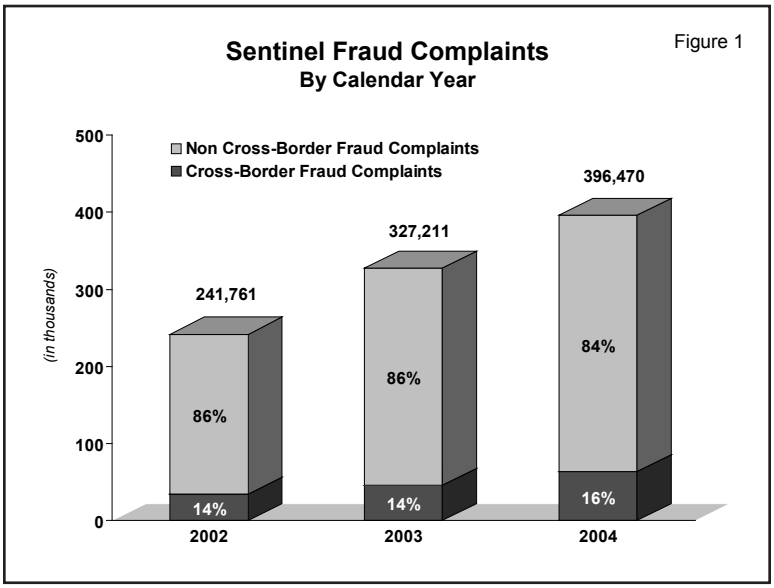
The US SAFE WEB Act strengthens FTC participation in a variety of international projects and networks. The FTC participates in many such projects and networks, including the International Consumer Protection Enforcement Network ("ICPEN"), the Mexico-U.S.-Canada Health Fraud Task Force ("MUCH"), and various regional enforcement task forces that include Canadian federal and provincial authorities and U.S. law enforcement. The Act would permit the FTC to contribute financially, within stated limits, to these joint projects. It also would permit the FTC to participate in staff exchanges with foreign counterparts. By permitting financial contributions and staff exchanges, the Act would improve the FTC's working relationships with such agencies and facilitate cooperative work necessary to protect consumers effectively in a global marketplace.

Part I of this Report describes the growing number of cross-border consumer complaints received by the FTC and the increasing number of FTC investigations with an international component. Part II describes some of the types of cases that are particularly likely to have an international component: spam, spyware, cross-border telemarketing, health advertising, and privacy and security. Part III discusses the harm that these illegal practices cause U.S. consumers. Part IV highlights certain key provisions of the proposed legislation and describes how they can help the FTC in its consumer protection investigations.

I. FTC Experience with Cross-border Complaints and Investigations in the Consumer Protection Area

American consumers are increasingly victimized by foreign con artists. A growing number of fraud complaints collected in *Consumer Sentinel* involve international transactions.[1] In 2004, 16 percent of the fraud complaints collected in *Consumer Sentinel* were reported to have involved either foreign businesses or foreign consumers (see Figure 1), compared to 13 percent in 2001 and less than one percent in 1995.[2]

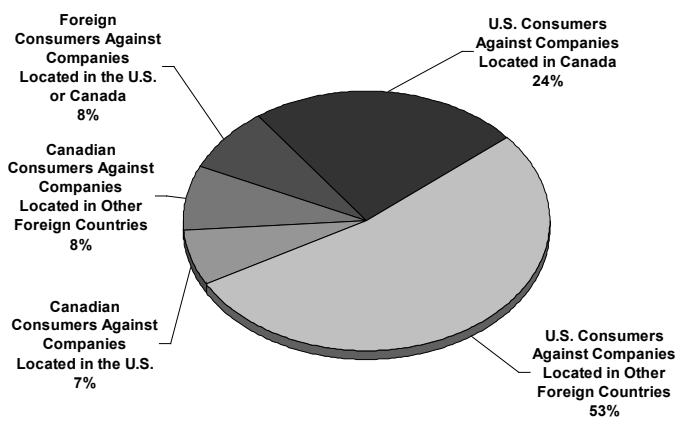
Figure 1



Seventy-seven percent of these complaints involved U.S. consumers complaining about foreign businesses.[3] (See Figure 2.) These complaints concern entities operating in many different countries, including Canada, the United Kingdom, Spain, Nigeria, Italy, the Netherlands, Greece, France, and Romania.

The 2004 cross-border complaints include more than 47,000 complaints by U.S. consumers against foreign companies (see Figure 3), complaining about transactions involving more than $92 million.[4] In the past three years, more than 100,000 U.S. consumers have lodged cross-border complaints.

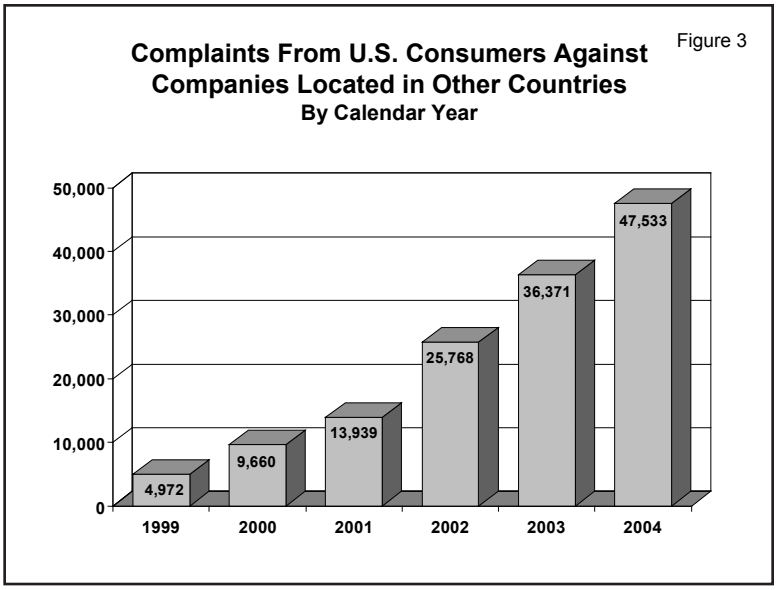
Figure 2



These statistics tell only part of the story. In many more instances, consumers do not know that their complaints are against foreign entities. Over one-third of the consumer fraud complaints collected in *Consumer Sentinel* do not reveal the location of the entity being complained about. The anonymity of the Internet, along with technological innovations

such as Caller-ID blocking and Voice over Internet Protocol ("VoIP"), can make it difficult for even the most well-informed consumers to determine the location of someone who is calling or emailing them.[5]

Figure 3



Indeed, consumers who think that they are dealing with a domestic entity may just as easily be dealing with a foreign one. An email "from" line may say "info@ebay.com," but in reality, the email could be coming from a "phisher" located on the other side of the world. A consumer might think she is giving her Social Security number to a bank's customer service representative calling her from a Richmond area code, but the person on the other end could be a thief sitting in Russia that has disguised his phone number using VoIP technology. A consumer might mail a check for an advance-fee loan offer he received from a telemarketer to a post office box in Vermont that is merely a mail drop for a boiler room across the border in Montreal.

Even when complaints involve U.S. consumers complaining about U.S. companies, Federal Trade Commission ("Commission" or "FTC") investigations often reveal that these U.S. companies use foreign intermediaries such as Internet Service Providers ("ISPs") to host websites or use foreign banks to hide their ill-gotten gains. Indeed, in several cases the FTC has found that domestic entities begin by using domestic intermediaries, but once they learn they are under investigation, they start using foreign ISPs to host their websites or foreign banks to hide their money. These fraudsters know that if they use a foreign ISP, it will be more difficult for the FTC to get information, and if they use a foreign bank, it will be more difficult for the FTC to get the money back to U.S. consumers.

II. The Faces of Cross-Border Consumer Complaints

The Undertaking Spam, Spyware, and Fraud Enforcement With Enforcers across Borders Act — the US SAFE WEB Act — would help the FTC fulfill its consumer protection mission in a range of investigations and cases.[6] This section highlights some of the particular areas in which the US SAFE WEB Act would assist the FTC in protecting consumers. These areas are often the subject of consumer complaints and FTC investigations and cases. They include spam, spyware, cross-border telemarketing, health fraud, and information security.

A. Spam

"I received a phishing e-mail from what I thought was [an online payment company.] In this e-mail I gave them my atm [sic] card number, pin number, and social security number. I was contacted by my bank telling me that fraudlent [sic] charges had been made from Romania. I obviously did not make the charges since I had been in Maryland the entire time."

– Consumer from Maryland[7]

"A company based in Brazil . . . has registered several websites. [The company] is forging the domain/email address of my non-profit organization . . . and sending tens of thousands of forged spam emails . . . ."

– Consumer from California

"I have received an email saying that I am a 2 million dollar winner in the British lottery. I actually believed it for a couple of days. Then I got suspicious and searched the internet for scams . . . . Imagine a working person finding out one day they have one [sic] a giant jackpot and then a couple of days later realizing you've been scammed. I could use 2 million dollars to pay off debts and realize some long-held wishes and dreams with that money. It broke my heart."

– Consumer from Texas

Spam is one of the most intractable consumer protection problems the FTC has ever faced. The extremely low cost of sending email makes it a very appealing marketing channel. Unfortunately, low cost, combined with anonymity, makes spam an ideal vehicle for con artists. Indeed, a 2003 FTC staff survey revealed that two-thirds of spam in its sample contained facial indications of falsity.[8]

In 1998, the FTC unveiled an initiative to compile and analyze spam for law enforcement purposes. The FTC encouraged consumers and others to forward spam to an FTC mailbox. This mailbox now receives 300,000 new spam messages a day. An examination of these messages shows that spam is not only being used to perpetrate traditional frauds such as offers for "herbal viagra," "free porn," or "free credit repair," but it is also being used as a vehicle for even more pernicious schemes, such as dissemination of viruses, spyware, and phishing schemes.

Federal Trade Commission

The FTC devotes significant resources to aggressive law enforcement against spammers. To date, the FTC has filed 71 spam-related cases against 209 individuals and companies. The biggest problem the Commission faces in bringing these cases is tracing the spammers. Spammers can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world. Indeed, as the FTC has repeatedly stated, "the path from a fraudulent spammer to a consumer's in-box typically crosses at least one international border and frequently several."[9]

The international nature of spam is well-documented. In responses to requests for information issued by the FTC, one U.S.-based ISP reported that in the first two months of 2004, 56 percent of the spam in its subscribers' in-boxes was routed through servers or proxies overseas.[10] According to the "Anti-Phishing Working Group," a public-private partnership focused on eliminating the fraud that results from phishing, almost two-thirds of the web hosts for phishing sites are located outside the United States.[11] FTC spam investigations bear out these statistics. A large number of FTC spam investigations have an international component. For example, FTC staff often find that sites advertised in spam emails are hosted by companies in Asia.

Some typical scenarios, using hypothetical facts based on a variety of real cases, include the following.[12]

- The investigative target registers as a European corporation with European bank accounts, uses a web hosting company in Asia, and channels money through a payment processor in the Caribbean. In some investigations, FTC staff finds evidence that ultimately shows the investigative target residing in the United States. When the Commission does not find a U.S. connection, it may be forced to abandon its investigation, even if the scheme targets U.S. consumers.
- FTC staff conducts months of investigation and traces a spammer to the Netherlands. Just before the Commission is about to serve the spammer with legal process, the spammer moves to Russia. FTC staff finds a Russian law enforcement agency willing to open its own investigation that could shut down the spammer. Unfortunately, because the Commission cannot share confidential information with the Russian agency, the Russian agency cannot act.

Although not a panacea for all of the problems faced in FTC spam investigations, the US SAFE WEB Act would give the FTC new tools to better trace spammers that operate, either themselves or through other entities, beyond the borders of the United States.

B. Spyware

"I went to a website where numerous spyware files were loaded onto my computer without my knowledge or consent. I was unalbe [sic] to stop the process once it started. I was able to remove all but [one]. My computer slowed to a crawl, it is unknown how much personal information was collected. I tried every spyware remover available without success. Ultimately my entire operating system had to be rebuilt. My computer was ruined by these slugs."

– Consumer from Ohio

"This company installed damaging spyware on my computer within minutes of booting my computer and accessing the internet. I NEVER gave permission to install anything on my computer, and did not even have time to click anything out of the ordinary. This spyware came out of nowhere. No one could uninstall it, despite many, many efforts by professionals. I lost valuable data and had to purchase a new hard drive because of this. This company stole my time, money, computer equipment and data from me, and does not identify its address on the internet."

– Consumer from California

The term spyware may be amorphous, but there is no doubt that its negative impact is real. It has been estimated that, excluding cookies, almost 70 percent of consumers' computers contain some form of spyware.[13] The serious damage that certain types of spyware can cause includes the following:

- Spyware can lead to identity theft when a "keystroke logger" captures all keystrokes the user types on the consumer keyboard, including passwords and PIN numbers.
- It can monitor and collect sensitive information, such as financial or medical information, from consumers.
- It can impair computer operation and performance. For example, spyware may cause computers to crash or can result in loss of Internet access.
- It can assert control over the operation of computers in ways that substantially limit the ability of consumers to use their computers. For example, it can change users' browser settings or home pages. In some cases, these changed settings may take the computer to adult content websites.[14]

The FTC hosted a workshop in April 2004 to explore issues associated with spyware. Several participants in this workshop emphasized that spyware was an international problem. In the words of one panelist: "The really bad people . . . operate in other places, and we're dealing with a global Internet."[15]

Federal Trade Commission

The FTC issued a staff report on spyware this past March, which summarized the international dimensions of this problem:

> "[G]iven the surreptitious nature of spyware, it often is difficult to ascertain from whom, from where, and how spyware has been disseminated . . . . [O]nce the distributor is identified, it may be located in a foreign jurisdiction, which can significantly complicate law enforcement efforts."[16]

The FTC has brought three enforcement actions so far involving spyware and has several more investigations in the pipeline.[17] In almost all of its investigations in this area, FTC staff encounters an international issue. For example, one FTC investigation into a particularly prevalent spyware program led to five investigative targets. The investigation included conducting detailed forensic work to figure out how the spyware programs worked, testing the software, proving consumer injury, and sending out investigative subpoenas to find the investigative targets. Months of painstaking investigation led to a finding that three of these targets were located offshore. Of these three targets, FTC staff had to abandon its investigation into two because the expenditure of resources required for pursuing these offshore targets was not justified, given the small likelihood of obtaining a meaningful remedy.

In other cases, FTC staff locates U.S.-based third parties, such as ISPs who provide web hosting services to foreign spyware operators or U.S.-based payment processors who process funds for them. However, as a result of negative experiences, the FTC often does not send Civil Investigative Demands ("CIDs") to these third parties because of the concern that they may tip off investigative targets. If the investigative targets become aware of FTC investigations, they can shut down websites and reappear to consumers in a different form – remaining one step ahead of law enforcement.

Finding spyware operators is even more difficult when they use foreign intermediaries, such as foreign ISPs, to host their websites. The FTC generally cannot compel foreign entities to produce evidence,[18] nor does it currently have any mechanism for sharing confidential investigative information with its foreign counterparts so that they can initiate investigations, either on their own or on the FTC's behalf.

Finally, in two separate spyware investigations, FTC staff found that separate entities had hired the same overseas software developer to write their pernicious spyware programs. Ideally, the FTC would initiate an investigation into the program developer, rather than the multiple buyers, but because this entity was abroad, the FTC has no effective mechanism for enforcing any remedy it would have been able to obtain.[19] And in any event, locating the entity, serving process, and litigating an action against a foreign defendant is extremely time-consuming and resource-intensive, given the FTC's limited tools. Although bringing foreign spyware operators

committing unfair and deceptive practices to justice will continue to be difficult even after the enactment of the US SAFE WEB Act, the Act can give the FTC additional tools that will increase the chance of success, as explained further in Section IV.

C. Cross-Border Telemarketing

"The charge [a Canadian-based telemarketer] made to my account caused about 50 checks to be returned because of non-sufficient funds. The bank charged me $875 in overdraft charges and hired a debt collector to collect the money from me and my husband. The debt collection service threatened to call the sheriff on us. [ ], one of the recipients of a check that bounced, threatened to report me to the District Attorney's office if I did not pay it by [a specific date]. Another merchant reported me to the postal inspectors for using the mail to send a worthless check. Our electricity was also turned off. I incurred $2,000 in lost money, non-sufficient check fees, and merchant fees. We could not afford to pay for my husband's cancer medicine. I felt as if I were going through a nervous breakdown."

- Consumer from Wisconsin

"The $249 [a Canadian telemarketer] has already stolen from me has had a hard impact on my family. My husband just passed away last year, at which time I was forced to file for bankruptcy. I was getting the supposed credit card [] to try to re-establish my credit. I have myself and my daughter to provide for, and I could not afford to lose that money."

- Consumer from Ohio

Although newer technologies such as spam and spyware have received a great deal of attention recently, telemarketing fraud continues to harm consumers. Canadian telemarketers continue to target the lucrative U.S. market with a host of scams.[20] Twenty-four percent of *Consumer Sentinel* cross-border fraud complaints in 2004 involved U.S. consumers complaining about Canadian companies. Of that 24 percent, over half who revealed how they were initially contacted said the same thing: They were contacted by telephone.

Typical telemarketing scams include free prize offers, "get-rich-quick" schemes and other investment opportunities, sale of foreign lottery tickets, phony charities, and advance-fee loans. These schemes can cheat consumers out of their life savings. Anyone with a phone can be victimized by telemarketing scam artists. Scammers may get a consumer's number from a telephone directory, a mailing list or what fraudsters call a "sucker list."[21] Sucker lists contain information about people who have responded to previous telemarketing solicitations. The lists are bought and sold by promoters. They are invaluable to scam artists, who believe that consumers who have been deceived once are vulnerable to additional scams.

Telemarketers constantly reinvent themselves. Previously, telemarketers set up boiler rooms in a fixed location with land lines and office space, but now a boiler room can be a few con men

in an SUV with prepaid disposable cell phones, bought with stolen credit cards. Plus, VoIP provides scam artists with some new tools. For example, using VoIP, telemarketers can blast huge numbers of voice mails to consumers at a very low cost. Imagine spam migrating from the in-box to a VoIP phone and you have "SPIT," spam over Internet telephony.[22]

Since 2000, the FTC has brought well over two dozen cross-border telemarketing cases. Unfortunately, with many telemarketing boiler rooms north of the border, cross-border telemarketing fraudsters can often shield themselves from U.S. law enforcement. The FTC cannot go directly into a Canadian court to shut down a fraudulent telemarketer and freeze its assets, as it can in the United States. Instead, pursuing the money in an FTC case requires a Canadian lawyer to argue the case in a Canadian court under U.S. Department of Justice supervision, while the FTC seeks a judgment in U.S. District Court. A new action must then be brought in Canada to enforce the final U.S. order.

Among other things, the US SAFE WEB Act would help target more resources toward foreign litigation by allowing the FTC to contribute additional staff and financial resources for foreign litigation of FTC matters. Although the process of returning money to U.S. consumers will still be difficult, the US SAFE WEB Act will provide helpful new tools.

D. Health and Weight-Loss Advertising

> *"The selling leaflet for this product was emphatic that the user would not need to be concerned with any of the following for miraculous slimming results: a) can eat or drink anything b) positively no dieting c) no exercising necessary d) no pills nded [sic] e) no surgery required . . . . The 'patch' is useless and no weight loss occured [sic] over the prescribed 28-day period."*
>
> *– Consumer from United Kingdom*

Like telemarketing fraud, cross-border advertising is not a new phenomenon. Advertisements in newspapers and magazines have always been disseminated across borders. But technological developments like the Internet and satellite television have brought with them a rapid increase in cross-border advertising. Of course, legitimate cross-border advertising itself is not the problem. Indeed, cross-border advertising is essential for businesses to promote their products to potential consumers and for consumers to make informed choices about the products they wish to purchase. Instead, the problem is rogue advertisers who have used technological developments to promote untruthful and misleading advertising to consumers around the world.

This is particularly true in the case of advertising for health and weight-loss products. The advertising of unproven and ineffective miracle cures for diseases and obesity has always been a problem. The FTC has long battled health claims for bogus and sometimes harmful health products marketed to consumers, including children.[23] With the latest data from the National

Center for Health Statistics indicating that over 60 million American adults - and over nine million children - are obese, consumers will continue to be vulnerable to these claims.[24]

The Internet and satellite TV have now given advertisers an unprecedented, inexpensive way to quickly reach millions of potential consumers worldwide. The Internet has become a busy global marketplace for promoters of dubious and sometimes harmful health and obesity-related products. For example, a health claims surf by the member countries of the International Consumer Protection and Enforcement Network ("ICPEN") identified more than 1,400 global websites making questionable claims for health-related products and services.[25]

Many FTC cases against false and deceptive advertising have an international component. Some scenarios the Commission faces, using hypothetical facts based on real cases, include the following:

- The FTC investigates a website advertising a bogus clinical arthritis cure treatment to consumers in the United States and elsewhere. The FTC learns that the defendants are based in Switzerland, and the "clinics" are located in Mexico. In some instances, the FTC and the Swiss and Mexican authorities cannot exchange information to bring these charlatans to justice because of statutory restrictions.
- The FTC files suit against the Australian-based promoters of a diet "patch," who claim that their patch causes substantial weight loss, boosts metabolism, suppresses appetite, and delivers its ingredients into the bloodstream more quickly and efficiently than pills. The FTC obtains an injunction and a judgment awarding consumer redress in the case. After the judgment is announced, the consumer protection agency in Australia contacts the FTC and requests the FTC's investigatory files so that it can file its own suit. The Australian lawsuit would benefit U.S. consumers because it would be difficult, time consuming, and costly to enforce the FTC's judgment in Australia. The FTC is not authorized, however, to turn over the materials it obtained through its CID to the Australian agency.
- The FTC sues the marketers of abdominal electronic muscle stimulation devices, who falsely advertise on the Internet and through infomercials that the devices will give users well-defined abdominal muscles (e.g., "rock hard," "six pack," or "washboard abs"). The FTC learns that the defendants are based in Europe and have transferred their assets there. There are hurdles to the FTC's obtaining sufficient information about these assets and to contributing the necessary resources to enforce any U.S. judgment, so that money can be returned to U.S. consumers.

Like other types of fraud, deceptive health advertising cheats consumers out of their money and dignity. Unlike other types of consumer fraud, it may cause harmful and long-lasting effects to a consumer's health. To battle this type of fraud effectively, the FTC needs the tools provided by the US SAFE WEB Act.

E. Information Security

> *"This company notified me that they were alerting my family and me that they may have sold our private and personal information to include ss#, checking account info, credit reports to criminals and we may be subject to identity theft, but they were 'sorry for the inconvenience.'"*
>
> *- Consumer from California*

Recent news reports about the unauthorized release of consumers' sensitive information by various data brokers, banks, and other companies demonstrate that if personal data about consumers is not adequately secured, it can fall into the wrong hands and cause serious harm to consumers. The consequences of security breaches can be severe, ranging from unauthorized charges to consumers' accounts and identity theft, to an increase in spam and "phishing" schemes. A 2003 FTC survey showed that over a one-year period nearly 10 million people – or 4.6 percent of the adult population – had discovered that they were victims of some form of identity theft.[26]

The FTC's primary goal is to encourage all companies to implement solid information security practices *before* a breach can occur. But when significant breaches do occur, the FTC will continue to determine whether they were caused by the failure to take reasonable steps to safeguard consumers' information. If so, the FTC will take appropriate action. Given the importance of information security to consumers, the FTC has made it one of its top law enforcement priorities, and it will dedicate even more resources to this critical issue.

Information security and privacy are increasingly global issues. U.S. consumers can and do reveal personal information to buy products and services from foreign websites. U.S. consumers are routinely asked to share their bank account and credit card numbers with telemarketers that could be calling from anywhere in the world. The US SAFE WEB Act would help address security breaches that occur when U.S. consumer data is located abroad.

For example, suppose the FTC is investigating a foreign company that sells vacations to U.S. consumers through a website. The company violates the FTC Act's prohibition on "unfair and deceptive acts or practices"[27] by failing to abide by its posted statement that it will "maintain reasonable safeguards in place to protect the security of consumer information." The FTC learns that a foreign agency is investigating the foreign company for violating a foreign law similar to

the FTC Act. Information exchange between the FTC and the foreign agency in this instance could streamline both investigations, avoid duplication of efforts, and give the FTC access to valuable information it would not otherwise have access to in the course of its investigation.

Currently, however, there are obstacles to sharing such information. The US SAFE WEB Act would overcome these obstacles.

III. Problems Caused by Cross-Border Schemes

The types of cross-border schemes discussed in Section II can cause significant harm to consumers. First and foremost, they cause monetary injury. Not only do consumer victims pay substantial sums to fraudulent telemarketers and spammers peddling bogus products, but consumers are often unwitting victims of identity theft and phishing scams that cause consumers significant economic harm.

The problem of consumer economic injury is exacerbated when these thieves hide their ill-gotten gains in offshore accounts. When investigative targets hide assets offshore, the FTC often has difficulty finding information about these assets. Even when the FTC does find the assets, it is difficult to preserve them pending a final judgment. And even if there is money left by the time the FTC obtains a judgment, it is difficult to enforce that judgment abroad. As a result, the Commission often finds that, when it obtains a judgment to make consumers whole, it cannot, as a practical matter, obtain that money to return it to consumers.

Second, not only can these schemes cause monetary harm, but they can deprive consumers of the benefits of new technologies. Spyware and viruses can cause significant disruption to personal and business computers. They can significantly slow down a user's browsing experience, shut down a user's Internet access, or even cause an individual or small business computer system to crash.

Third, in the area of health fraud, not only do these schemes lead consumers to waste millions of dollars on useless products, but they can cause even greater harm by leading people to delay proper medical treatment.[28] This is especially true in cases involving supposed miracle cures for diseases such as cancer and AIDS.

Finally, cross-border scams dilute consumer confidence in the global marketplace, leading consumers to conclude that they should only do business with known, local merchants. Indeed, as one consumer said in her spyware complaint to the FTC, "this experience indicates to me that the Internet is not a secure or safe place to do business, since large companies can send out

malicious programs to virtually take over a consumer's computer, and possibly steal confidential personal information." If the promise of the global marketplace is to be fully realized, governments must assure consumers that they are working to protect them in that marketplace.

Failure to address the cross-border problem now will only make it worse in the future. If cross-border con artists succeed in evading law enforcement, others will emulate them, structure their operations to include an international component, and cheat more and more consumers for larger amounts of money. Giving the FTC new tools in this area would send a message to these con artists, and the FTC's use of these tools would help deter wrongful conduct.

IV. The US SAFE WEB Act

The FTC has been working aggressively within the existing legislative framework to combat spam, spyware, telemarketing fraud, and other types of unfair and deceptive practices, using a variety of approaches. On the enforcement front, the FTC has brought numerous cases in federal court against illegal spammers,[29] spyware operators,[30] and telemarketers.[31] In the past five years, the FTC has filed approximately 90 cases in federal courts involving foreign defendants, foreign consumers, evidence located abroad, or offshore assets. These cases have been filed against defendants based in Australia, Canada, Cyprus, Germany, Hong Kong, Mexico, the Netherlands, Peru, Spain, Switzerland, Taiwan, and the United Kingdom. They involve assets concealed in such offshore jurisdictions as the Bahamas, the Cayman Islands, the Cook Islands, the Isle of Man, and St. Kitts & Nevis. Through these cases, the FTC has obtained millions of dollars in redress for U.S. fraud victims and worked with criminal law enforcement agencies to punish wrongdoers. The FTC also has distributed redress funds to consumer victims located in over 100 countries.[32]

Furthermore, the FTC has cooperated with its international counterparts to try to address the challenges posed by these cross-border scams. The FTC participates in several multilateral enforcement networks, such as ICPEN[33] and the London Action Plan on international spam enforcement cooperation.[34] The FTC has entered into bilateral cooperation agreements with agencies in Australia, Canada, Ireland, Mexico, and the United Kingdom and executed memoranda of understanding on spam enforcement with agencies in Australia, the United Kingdom, and Spain.[35] In Canada, the Commission participates in several regional consumer protection enforcement task forces, which include civil and criminal law enforcement agencies from both sides of the border.[36] The FTC also participates in several international education, monitoring, and enforcement projects.[37]

But these efforts are not as effective as they could be. Despite its successes, the FTC faces daunting challenges in battling new, sophisticated high-tech frauds and in stemming the growth of more traditional types of cross-border schemes against consumers. Many of these challenges reflect the shortcomings of a legal framework developed when consumer protection was a predominantly domestic concern. Though scams may be borderless, in many instances, the FTC's ability to share information and take action are limited by geographic boundaries. Even under the agreements and memoranda of understanding described above, the FTC can only share very limited categories of information. In the emerging global marketplace, the legal framework governing the FTC should be expanded to allow the FTC to act with effectiveness and dispatch to protect American consumers. Indeed, recent Congressional hearings on spam, spyware, and identity theft have emphasized the need for improvements to the FTC's law enforcement powers to combat law violations in these areas.[38]

To address these challenges, the FTC is proposing several legislative recommendations to Congress in the form of a proposed bill — the US SAFE WEB Act. The proposed legislation would improve the FTC's ability to combat the types of schemes discussed in this report in four main ways. It would (1) allow the FTC to leverage the resources of its foreign counterparts by improving its ability to cooperate with them in specific cases and investigations; (2) improve the FTC's information-gathering capabilities; (3) strengthen the FTC's ability to obtain consumer redress; and (4) allow the FTC to strengthen its enforcement cooperation networks.[39]

A. Improving International Cooperation in Cases and Investigations

The FTC currently is not authorized to share confidential information that it obtains in consumer protection investigations with foreign law enforcement, although a provision of the FTC Act allows routine sharing of that information with U.S. federal and state law enforcement.[40] The FTC also does not have the authority to provide investigative assistance to foreign agencies that are investigating consumer protection violations that harm U.S. consumers. These limitations affect the FTC's ability to protect U.S. consumers effectively. The following scenario illustrates some of the problems the Commission faces, and how the US SAFE WEB Act would fix them:

The scenario: The FTC obtains a court order against a spammer who was defrauding U.S. consumers by selling bogus miracle cures. The order shuts down the websites operated by the spammer. Afterwards, the FTC learns that the spammer has an affiliate that is perpetrating the same scam from Sweden, targeting both U.S. and foreign consumers. Despite the FTC's lawsuit, U.S. consumers continue to be bombarded by this spam.

Current limitations: The Swedish authority decides to take action against the affiliate, and asks the FTC for information the FTC obtained during its investigation to aid in Swedish law enforcement efforts. Under current law, the FTC cannot share the information it obtained pursuant to its main investigatory tool, the CID, with its foreign counterpart. The Swedish authority also asks the FTC to obtain testimony from the U.S.-based spammer about the Swedish affiliate's operations. Under current law, the FTC has no mechanism for obtaining this type of information and providing it to the Swedish authority.

US SAFE WEB Act: If the US SAFE WEB Act were enacted, the FTC would be able to share the information it had gathered in its investigation with the Swedish authorities to allow them to bring their own action against the affiliate spammer. Under the new legislation, the FTC could also send a CID to the U.S.-based spammer to investigate the foreign affiliate's conduct. This would benefit U.S. consumers by helping the Swedish authority to shut down the affiliate's websites.

Our proposed provisions in this area track provisions that many federal agencies, such as the Securities and Exchange Commission ("SEC"), Commodities Futures Trading Commission ("CFTC"), and federal banking agencies already have.[41] As with these agencies, provisions allowing the FTC to share information and provide investigative assistance in consumer protection cases will greatly help protect U.S. consumers.

B. Improving Information-Gathering Capabilities

When the FTC investigates fraud and deception, it often relies on CIDs sent to third parties such as banks, credit card companies, payment processors, commercial mail receiving agencies, ISPs, and domain registrars, to obtain information about particular targets. The success of FTC action against spam, spyware, and telemarketing frauds often depends on keeping investigations confidential without prematurely tipping off investigative targets. Once notified of FTC action, targets in these cases can disappear and move assets offshore, beyond the reach of U.S. courts. This makes it much more difficult to obtain redress for U.S. fraud victims. Thus, the FTC seeks to improve its ability to obtain more information from third parties without tipping off investigative targets.

Existing federal legislation requires agencies seeking certain information from financial institutions and ISPs to provide notice to investigative targets. However, Congress has always recognized that in some situations, the needs of law enforcement justify delaying that notice for a limited time. A provision of the US SAFE WEB Act, modeled on existing securities law, would clarify that one of those situations is to prevent the concealment or expatriation of assets that are likely to be needed by the FTC for consumer redress.

Even when no federal law requires notice to investigative targets, many third parties have stated that they will provide such notice before they will share information with the FTC in response to a CID. Currently, the FTC has no mechanism to require these third parties to delay such notice. Because of the concern that such notice would tip off investigative targets, the FTC often does not send the CIDs, thus losing a potential source of information in FTC investigations.

The following scenario illustrates how this issue unfolds in FTC cases, and how the US SAFE WEB Act would provide a mechanism to prevent the transfer of assets offshore:

The scenario: The FTC is investigating a telemarketing scheme that preys on consumers by inducing them to purchase bogus "advance-fee" credit cards using a network of telemarketing boiler rooms in Canada and outsourced fulfillment and customer service centers around the world. The FTC finds that the promoters of the scheme, a corporation and two individuals, have accounts at a U.S. bank and wants to obtain financial information from the bank. If the FTC serves a CID on the bank, the FTC is required to notify the individual targets unless a court orders otherwise, and, although not required to do so, the bank may voluntarily choose to notify the corporate target. The targets may then move assets offshore to Caribbean banks.

Current limitations: Currently, there are two restrictions on the FTC's ability to keep CIDs confidential (1) third parties sometimes will disclose the existence of a CID to a customer that is an investigative target; and (2) the FTC is required by law, in certain cases, to provide notice to investigative targets when it issues a CID to certain financial institutions and ISPs.

US SAFE WEB Act: If the US SAFE WEB Act were enacted, the FTC, through its own attorneys, would be able to seek a court-ordered delay of notice if it can show reason to believe that disclosure of the CID may cause the target to transfer assets or records outside the United States or engage in other specified adverse actions. This court-ordered delay would allow the FTC to keep the CID and its investigation confidential for a limited period of time so that it could obtain the information from the bank without tipping off the target.

These proposals track similar provisions in the Securities Exchange Act,[42] and carefully balance law enforcement interests with privacy interests: in all cases in which the FTC seeks a mandate that third parties keep CIDs confidential, the FTC would be required to obtain a court order, and the confidential treatment would be temporary.

C. Consumer Redress

Key to an effective anti-fraud program is depriving wrongdoers of their ill-gotten gains, reducing the incentives to engage in fraud, and returning the money to consumers. Returning money to consumers reduces their injury and increases their confidence in the marketplace.

Among the changes the Commission is recommending is a provision expressly confirming the Commission's authority to take action in appropriate cross-border cases, including the authority to provide restitution to U.S. and foreign consumers injured by cross-border consumer protection law violations. The following scenario illustrates the benefit of clarifying this authority:

The scenario: The FTC files a lawsuit against the U.S.-based operators of an investment opportunity scam. The scam has thousands of victims in the U.S. and around the world. The defendants challenge the FTC's authority to recover funds for the injuries to foreign consumers and provide them with monetary redress. The defendants file an appeal with a U.S. Court of Appeals. The FTC spends considerable time and resources litigating this issue.

Current limitations: Although the FTC Act and federal case law make clear that the FTC may use its authority in cross-border cases, the FTC has increasingly faced legal challenges to its authority to take action in cross-border matters, particularly in the area of restitution or consumer redress.

US SAFE WEB Act: If the US SAFE WEB Act were enacted, the FTC could quickly dispose of spurious challenges to its authority to take action and obtain remedies, including restitution. By expressly confirming the availability of remedies under the FTC Act in cross-border transactions, Congress can protect Americans from foreign fraud operators and prevent the United States from becoming a haven for cross-border fraud operators targeting victims abroad. It also can send a strong signal to foreign courts considering whether to enforce an FTC money judgment when there are foreign as well as U.S. victims, that the United States is willing to pursue actions that benefit foreign consumers. Similarly, it can influence foreign governments considering legislative changes and foreign law enforcers considering actions benefitting U.S. consumers.

Moreover, the Commission increasingly is facing significant obstacles in recovering assets from defendants who have placed them abroad, beyond the reach of U.S. courts. The Commission therefore also seeks legislative changes helping to target more resources toward foreign litigation to facilitate recovery of offshore assets to benefit victimized U.S. consumers.

D. Strengthening Enforcement Relationships

The FTC participates in many international projects to combat cross-border consumer protection law violations, as outlined above. Often, it would be helpful for the FTC to provide monetary assistance to support cooperative projects of such groups. The FTC's legislative proposals seek to address existing restrictions in this area. The following scenario is illustrative:

The scenario: At a meeting of ICPEN, a network of consumer protection enforcement agencies from over 30 countries, agency representatives share their experiences about spyware enforcement. From their discussion, they learn that many of them have brought enforcement actions involving different spyware purveyors. Discussions reveal that many of these companies have all bought their pernicious software from a spyware kingpin. No one knows the location of this kingpin. ICPEN members decide to pool their resources to hire someone to work with individual countries on investigations.

Current limitations: The FTC cannot currently contribute resources to hire an ICPEN consultant. Various appropriations statutes prohibit the FTC from using appropriated funds to pay for a Commission, council, board or similar group that does not have prior and specific statutory approval to receive financial support.[43]

US SAFE WEB Act: The proposed US SAFE WEB Act contains a specific provision authorizing the expenditure of funds for ICPEN and other similar organizations, thereby satisfying the requirement that such organizations be specifically authorized by statute to receive financial support. If the US SAFE WEB Act were enacted, the FTC could provide monetary support for hiring the ICPEN consultant.

The SEC has been granted appropriations toward the funding of the International Organization of Securities Commissions.[44] A grant of authority to the FTC to make similar expenditures would help facilitate cooperative work necessary to effectively protect consumers in a global marketplace.

V. Conclusion

The proposed US SAFE WEB Act draws on established models for international cooperation pioneered by agencies such as the SEC and CFTC. Nearly fifteen years ago, Congress expanded the SEC's powers to cooperate with foreign authorities.[45] At the time, the SEC faced challenges analogous to those faced by the FTC today. According to a Congressional report,

> [T]he internationalization of the world's securities markets is a trend that is likely to continue at a rapid pace. The major forces driving this trend appear to be: rapid technological advances in communications and computer technology [and] the growing economic interdependence between the U.S. and its major trading partners . . . Therefore, securities regulators in each nation must work with their foreign counterparts to seek coordinated international solutions to assure fairer as well as more efficient market operations across borders.[46]

Since 1990, the SEC has had statutory authority to gather and share relevant information with its foreign counterparts, which has significantly helped the SEC protect American investors. Congress has given the CFTC similar powers and mechanisms for cooperation with foreign authorities.[47] In implementing the enhanced powers given them by Congress, these financial regulatory agencies have established a model for international cooperation that provides for flexibility and speed. Like the SEC and CFTC, the FTC needs timely and flexible means of cooperating with its foreign counterparts to protect consumers in a global marketplace.

In short, the types of cross-border schemes discussed in this report result in harm to consumers that is real and widespread: spam that inundates their in-boxes and entices them into fraudulent schemes, spyware that steals their data and crashes their computers, telemarketing and health claims that prey on their weaknesses, and data theft that can steal their very identities. The FTC works aggressively within the existing legal framework to battle these schemes. However, new legislation is vital to overcome existing obstacles to information sharing, improve the FTC's ability to gather information, enhance the FTC's ability to take effective action in cross-border cases, and strengthen the FTC's ability to cooperate with foreign authorities. These measures will improve the FTC's ability to make the web, and the global marketplace, a safer place for U.S. consumers.

Endnotes

1. *Consumer Sentinel* is a database of consumer fraud and identity theft complaints maintained by the FTC. Complaints are input into the database from many sources and are accessible to more than 1,300 law enforcement agencies in the United States, Canada, and Australia. The database currently contains over 2.3 million fraud and identity theft complaints. *See* http://www.consumer.gov/sentinel.
2. *See* Federal Trade Comm'n Report, "Cross-Border Fraud Trends," at 5 (Mar. 6, 2005), *available at* http://www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/Cross-BorderCY-2004.pdf; *see also* Timothy J. Muris, "Prepared Remarks at the Fordham Corporate Law Institute's Twenty-Ninth Annual Conference on International Antitrust Law and Policy," at n.55 (Oct. 31, 2002), *available at* http://www.ftc.gov/speeches/muris/021031fordham.pdf.
3. *See* "Cross-Border Fraud Trends," *supra* note 2, at 7.
4. *See id*. at 8, 12.
5. For information about how VoIP works, see http://www.fcc.gov/voip.
6. The FTC Act authorizes the FTC "to make annual and special reports to the Congress and to submit therewith recommendations for additional legislation. . . " 15 U.S.C. § 46(f).
7. This complaint and the other consumer complaints quoted in this report were culled from the *Consumer Sentinel* database (*see supra* note 1) and consumer declarations that have been filed in support of FTC legal pleadings. The FTC's treatment of information provided by consumers is described in the FTC's Privacy Policy, *available at* http://www.ftc.gov/ftc/privacy.htm.
8. *See* Press Release, "FTC Measures False Claims Inherent in Random Spam" (Apr. 29, 2003), *available at* http://www.ftc.gov/opa/2003/04/spamrpt.htm.
9. *Spam (Unsolicited Commercial E-Mail): Hearing Before the Senate Comm. on Commerce, Science and Transp.*, 108th Cong. (2003) (statements of Orson Swindle and Mozelle Thompson, Commissioners, Federal Trade Comm'n).
10. Federal Trade Comm'n, "National Do Not Email Registry: A Report to Congress," at n.45 (Jun. 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.
11. Anti-Phishing Working Group, "Phishing Activity Trends Report" (Mar. 2005), *available at* http://antiphishing.org/APWG_Phishing_Activity_Report_March_2005.pdf.
12. To preserve the confidentiality of investigative information, this report uses scenarios in which facts from different cases or investigations are combined and/or country names have been changed.
13. Webroot Software, Inc., "State of Spyware: Q1 2005" (May 2005), *available at* http://www.webroot.com/stateofspyware.
14. Federal Trade Comm'n Staff Report, "Monitoring Software on Your PC: Spyware, Adware, and Other Software," at 8-11 (Mar. 2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.
15. Federal Trade Comm'n Workshop, "Monitoring Software on Your PC: Spyware, Adware, and Other Software," Tr. at 190 (Apr. 19, 2004), *available at* http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf.
16. *See* "Monitoring Software on Your PC: Spyware, Adware, and Other Software," *supra* note 14 at 19.
17. *FTC v. Seismic Entm't Prods., Inc.*, No. 04-377-JD (D.N.H. filed Oct. 6, 2004); *FTC v. Maxtheater, Inc.*, No. 05-CV-0069-LRS (E.D. Wash. filed Mar. 8, 2005); *FTC v. Trustsoft*, No. 05-1905 (S.D. Tex. filed Jun. 1, 2005).
18. The FTC Act authorizes service of a CID on foreign citizens of foreign nations in accordance with the Federal Rules of Civil Procedure's rules on service of process. 15 U.S.C. § 57b-1(c)(7)(B). As a practical matter, however, the process is time-consuming and cumbersome and unlikely to yield evidence in a timely manner, if at all. Even if the FTC properly serves a CID on a foreign national over whom a U.S. court has personal jurisdiction, if that foreign national refuses to comply, the FTC's only remedy is to file an action for compliance in the United States District Court for the District of Columbia. 15 U.S.C. § 57b-1(c)(7)(c)).

Contempt of court generally is not an extraditable offense, and thus, there would be no feasible way to compel responses. *See* Restatement (Third) of the Foreign Relations Law of the United States § 475 cmt. c (1987); Treaty on Extradition, Dec. 3, 1971, U.S.-Can., 27 U.S.T. 983; Extradition Treaty, Jun. 8, 1972, U.S.-U.K., 28 U.S.T. 227; Extradition Supplementary Treaty, Jun. 25, 1985, U.S.-U.K. T.I.A.S. No. 12050; Treaty on Extradition, May 14, 1974, U.S.-Austral., 27 U.S.T. 957; Extradition Treaty, May 4, 1978, U.S.-Mex., 31 U.S.T. 5059; Treaty Concerning Extradition, Jun. 20, 1978, U.S.-Ger. (FRG), 32 U.S.T. 1485.

19. *See id.*, explaining that the remedy for non-compliance with a U.S. court order is contempt of court, which is not an extraditable offense.

20. Of course, Canada is not the only country from where foreign telemarketers call U.S. consumers. Telemarketing scams emanate from Latin America and other places as well.

21. *See* Federal Trade Comm'n Facts for Consumers, "Telemarketing Recovery Scams," *available at* http://www.ftc.gov/bcp/conline/pubs/tmarkg/recovery.pdf.

22. *See* Deborah Platt Majoras, "State of the FTC" at 22 (Mar. 28, 2005), *available at* http://www.ftc.gov/speeches/majoras/050328stateofftc.pdf.

23. In 1999, the FTC launched Operation Cure-All to combat bogus claims for products and treatments touted as cures for various diseases. Information about Operation Cure-All initiatives and cases is available on the FTC's website at http://www.ftc.gov/bcp/conline/edcams/cureall/coninfo.htm. The Commission continues to be active in bringing enforcement actions against false health claims. *See Parents Be Aware: Health Concerns about Dietary Supplements for Overweight Children: Hearing Before the Subcomm. on Oversight and Investigations, House Comm. on Energy and Commerce*, 108th Cong. (2004) (statement of J. Howard Beales III, Director, Bureau of Consumer Protection, FTC); *Dietary Supplements: Hearing Before the Senate Comm. on Commerce, Science, and Transp.*, 108th Cong. (2003) (statement of J. Howard Beales III, Director, Bureau of Consumer Protection, FTC).

24. *See* Centers for Disease Control and Prevention, "Overweight and Obesity: Home," *available at* http://www.cdc.gov/nccdphp/dnpa/obesity/.

25. Press Release, "Consumer Protection Agencies Combat Cross-Border Fraud" (Sept. 24, 2002) (reporting results of global health claims surf), *available at* http://www.ftc.gov/opa/2002/09/imsnsydney.htm.

26. Federal Trade Comm'n, "Identity Theft Survey Report" (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

27. *See* 15 U.S.C. § 45(a).

28. *See* "Miracle Health Claims: Add a Dose of Skepticism," *available at* http://www.ftc.gov/bcp/conline/pubs/health/frdheal.htm.

29. *See* FTC Spam Press Room, *available at* http://www.ftc.gov/bcp/conline/edcams/spam/press.htm.

30. *See supra* note 17.

31. *See* Press Release, "FTC Continues Aggressive Fight Against Telemarketing Fraud and Abuse" (Apr. 28, 2005), *available at* http://www.ftc.gov/opa/2005/04/telemarkenf.htm.

32. *See* Deborah Platt Majoras, "Keynote Address Before OECD Workshop on Dispute Resolution and Redress" (Apr. 19, 2005), *available at* http://www.ftc.gov/speeches/majoras/050419oecdworkshop.pdf.

33. ICPEN is a group of consumer protection enforcement agencies from 33 countries plus the European Commission and the Organisation for Economic Co-operation and Development that shares information about cross-border commercial activities that may affect consumer interests, and encourages international cooperation among law enforcement agencies. *See* http://www.icpen.org. Many ICPEN members participate in *econsumer.gov*, a public website hosted by the FTC, where consumers can file cross-border e-commerce complaints online, making them accessible to law enforcement agencies in the member countries. The site is available in English, French, Spanish, German, and Korean. Complaints from *econsumer.gov* help the FTC identify trends and wrongdoers on an international level.

34. The London Action Plan consists of 28 spam enforcement agencies from 20 countries and several private sector representatives that meet periodically via teleconference to share information, trends, and investigative techniques about spam. *See* Press Release, "FTC, International Agencies Adopt Action Plan on Spam Enforcement" (Oct. 12, 2004), *available at* http://www.ftc.gov/opa/2004/10/spamconference.htm.

35. *See Agreement Between the Federal Trade Commission of the United States of America and the Australian Competition & Consumer Commission On the Mutual Enforcement Assistance in Consumer Protection Matters* (Jul. 20, 1999), *available at* http://www.ftc.gov/opa/2000/07/usaccc.htm; *Agreement Between the Government of the United States of America and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices Laws*, Trade Reg. Rep. (CCH) ¶ 13,503 (1995), available at http://www.usdoj.gov/atr/public/international/docs/uscan721.htm; *Memorandum Of Understanding On Mutual Enforcement Assistance In Consumer Protection Matters Between The United States Federal Trade Commission And Ireland's Office of the Director of Consumer Affairs* (Oct. 9, 2003), *available at* http://www.ftc.gov/opa/2003/10/irelandcb.htm; *Memorandum of Understanding On Mutual Assistance In Consumer Protection Matters Between the Federal Trade Commission of the United States of America and the Procuraduria Federal Del Consumidor (Office of the Federal Attorney for Consumer Protection) of the United Mexican States* (Jan. 27, 2005), *available at* http://www.ftc.gov/opa/2005/01/memunderstanding.htm; *Memorandum Of Understanding On Mutual Enforcement Assistance In Consumer Protection Matters Between The Federal Trade Commission Of The United States of America And Her Majesty's Secretary of State for Trade And Industry And The Director General Of Fair Trading In The United Kingdom* (Oct. 31, 2000), *available at* http://www.ftc.gov/opa/2000/10/ukimsn.htm; *Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters among the Following Agencies of the United States, the United Kingdom, and Australia: the United States Federal Trade Commission, the United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of State for Trade And Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority* (Jul. 2, 2004), *available at* http://www.ftc.gov/opa/2004/07/mou.htm; and *Memorandum of Understanding On Mutual Enforcement Assistance In Commercial Email Matters Between the Federal Trade Commission of the United States of America and the Agencia Espanola de Proteccion de Datos* (Feb. 24, 2005), *available at* http://www.ftc.gov/opa/2005/02/spainspam.htm.

36. The FTC is a member of several U.S.-Canada cross-border mass marketing fraud enforcement task forces. Each task force focuses on cases with a nexus in a particular Canadian province or provinces, as follows: the Alberta Partnership Against Cross-Border Fraud (Alberta); the Atlantic Partnership (New Brunswick, Newfoundland, Nova Scotia, and Prince Edward Island); Project Emptor (British Columbia); Toronto Strategic Partnership (Ontario); and Vancouver Strategic Alliance (British Columbia).

37. The FTC participates in international surf days, law enforcement sweeps, international technical assistance (including Internet investigations training seminars), and consumer education. The FTC also participates in bilateral and multilateral teleconferences and meetings to educate other countries on fighting cross-border fraud. For example, FTC staff coordinates a monthly Informal Panamerican Dialogue with Latin American consumer protection agencies.

38. *See Spyware: Hearing Before the Senate Comm. on Commerce, Science, & Transp.*, 108th Cong. (2005) (statement of Senator Smith and statement of Senator Allen); *Privacy: Hearing Before the Senate Comm. on Commerce, Science, & Transp.*, 108th Cong. (2005) (statement of Jon Leibowitz, Commissioner, Federal Trade Commission); *Spam (Unsolicited Commercial E-Mail): Hearing Before the Senate Comm. on Commerce, Science and Transp.*, 108th Cong. (2003) (statement of Orson Swindle and Mozelle Thompson, Commissioners, Federal Trade Commission).

39. For a detailed summary of each of the US SAFE WEB Act's provisions, see Federal Trade Comm'n Submission to Congress, "Briefing Materials" (Jun. 2005).

40. The Commission cannot disclose "documentary material, tangible things, reports or answers to questions and transcripts of oral testimony" that are "received by the Commission pursuant to compulsory process in an investigation" without the consent of the person who submitted the information, except as specifically provided. 15 U.S.C. § 57b-2(b)(3)(C); 16 C.F.R. § 4.10(d); *see also* 15 U.S.C. § 46(f); 15 U.S.C. § 57b-2(b)(6).

41. 15 U.S.C. § 78x(c));15 U.S.C. §§ 78u(a)(2) and (b); 7 U.S.C. § 12(e); 7 U.S.C. § 16(f); 12 U.S.C. § 3109(a)-(b); 12 U.S.C. § 1818(v)(2).
42. *See* 15 U.S.C. § 78u(h).
43. *See id.*
44. *See* Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, Division B, Title V, 118 Stat. 2809, *2910.
45. *See* Securities Acts Amendments of 1990, Pub. L. 101-550 (1990).
46. H.R. Rep. No. 101-240 at 2-3 (1990), *see* 1990 U.S. Code Cong. and Adm. News 3889-90.
47. H.R. Conf. Rep. No. 978, 102d Cong., 2d Sess. 70-71 (1992).

FEDERAL TRADE COMMISSION
FOR THE CONSUMER
1.877.FTC.HELP
FTC.GOV