An Explanation of the Provisions of the US SAFE WEB Act

This document summarizes and explains the provisions of the proposed US SAFE WEB Act of 2005: Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders Act.[1] The box below shows where each particular provision of the Act is discussed.

The US SAFE WEB Act would greatly aid the Federal Trade Commission (the "Commission" or "FTC") in its efforts to protect U.S. consumers from global fraud by (1) improving the FTC's ability to cooperate with foreign counterparts in specific cases and investigations; (2) improving the FTC's ability to gather information; (3) enhancing the FTC's ability to obtain monetary consumer redress; and (4) strengthening the FTC's enforcement cooperation networks.

US SAFE WEB Act: Section-by-Section Key

I. Improving the FTC's Investigative Cooperation with Foreign Authorities

A. Broadening Reciprocal Information Sharing

US SAFE WEB Act §§ 4(a), 6(a): Allows the FTC to share confidential information in its files in consumer protection matters with foreign law enforcers, subject to appropriate confidentiality assurances. **Similar to** longstanding SEC, CFTC, and federal banking agency authority. **Needed to** allow the FTC to share information with foreign agencies to help them halt fraud, deception, spam, spyware and other consumer protection law violations targeting U.S. consumers. Also **needed** for the FTC to obtain, in return, foreign information required to halt such illegal practices.

Currently, the FTC cannot share confidential information, such as that obtained through its civil investigative demand ("CID") process, with foreign law enforcement, as it does with other federal, state, and local law enforcement agencies.[2] The FTC's inability to share such information with its foreign counterparts has hurt U.S. consumers. The US SAFE WEB Act would allow the FTC to share such information with its foreign counterparts, subject to appropriate confidentiality assurances.[3] The US SAFE WEB Act provision is modeled on provisions in other statutes giving the Securities and Exchange Commission ("SEC"),[4] the Commodity Futures Trading Commission ("CFTC"),[5] and federal banking agencies[6] authority to share such information with foreign counterparts.

The existing limits on sharing compelled or confidential information hinders the FTC's law enforcement efforts and can hurt U.S. consumers. Sometimes, the FTC and a foreign agency investigate the same targets. If the FTC had the authority to share more complete information about the target, this could not only streamline parallel investigations, but actually facilitate specific enforcement actions. For example, suppose that the FTC and a Dutch law enforcement agency are investigating the same Dutch spyware programmer whose pernicious spyware is affecting U.S. and foreign consumers.[7] It would make sense for the FTC to share with the Dutch agency information it has obtained by CID from a U.S.-based Internet Service Provider ("ISP"). This way, the Dutch agency can take immediate action in a Dutch court to shut down the spyware operation, thus benefitting U.S. consumers. Without the US SAFE WEB Act, the FTC is only allowed to share that information if the U.S.-based ISP provides consent to the FTC to share its CID responses with the Dutch authority. The Commission's experience is that in many such

cases, this will not happen – sometimes because the CID recipient is itself involved in the scam and sometimes because the CID recipient has liability or customer relations concerns about providing consent.

In other cases, more complete information sharing could help avoid duplication of efforts and may speed up investigations. It could also increase the quantity and quality of evidence against an investigative target. Authorizing the FTC to share such information will also encourage foreign law enforcement agencies to provide reciprocal information sharing to the FTC, and encourage foreign states to authorize increased information sharing with the FTC.

B. Expanding Investigative Cooperation

US SAFE WEB Act § 4(b) (adding FTC Act § 6(j)): Allows the FTC to conduct investigations and discovery to help foreign law enforcers in appropriate cases. **Similar to** longstanding SEC, CFTC, and federal banking agency authority. **Needed to** allow the FTC to obtain information for foreign agencies' actions to halt fraud, deception, spam, spyware, and other consumer protection law violations targeting U.S. consumers. Also **needed** to help the FTC to obtain, in return, foreign investigative assistance in FTC cases.

In some cases, effective enforcement cooperation demands that the Commission reach beyond information already in its files and gather new information on behalf of foreign law enforcement agencies. This would both assist foreign investigations, which often directly benefit U.S. consumers, and encourage the foreign law enforcement agencies to provide reciprocal assistance to the FTC. The US SAFE WEB Act would give the Commission the authority to conduct investigations and obtain evidence on behalf of its foreign counterparts if it determines that such actions are in the public interest.[8] The proposed Act would also authorize the FTC to negotiate and conclude international agreements when required as a condition of reciprocal assistance.

1. Conducting Investigations Using Civil Investigative Demands

Under current law, the FTC is not authorized to use its main investigatory tool, the CID, on behalf of its foreign counterparts to obtain information for use in their investigations.[9] This is true even when the foreign law enforcement agency is investigating conduct that harms U.S. consumers.[10] The US SAFE WEB Act contains a provision that would allow the FTC to issue CIDs to assist its foreign counterparts. The US SAFE WEB Act provision is modeled on existing statutes granting the SEC, CFTC, and federal banking agencies authority to conduct investigations on request from foreign counterpart agencies.[11]

In many instances, providing investigative assistance to foreign counterparts would benefit U.S. consumers. For example, suppose a Canadian agency is investigating a Canadian telemarketer selling bogus lottery tickets to elderly U.S. consumers. The Canadian agency might ask the FTC to issue CIDs to obtain information from a U.S.-based payment processor. Such information would assist the Canadian agency in its investigation, which would in turn benefit U.S. consumers at little cost to the FTC. However, without the US SAFE WEB Act, if the FTC were not itself investigating the Canadian company, it would not have the authority to issue the CIDs.

The Commission's current lack of authority to use CIDs on behalf of foreign enforcement agencies is troubling because assisting a foreign agency's in-progress investigation will, in some cases, protect U.S. consumers more quickly, more effectively, and at far less cost than the FTC's undertaking its own action. The US SAFE WEB Act provision on investigative assistance would give the FTC the discretion whether (and to what extent) to provide assistance, and would require the FTC to consider certain criteria, including the public interest of the United States and the availability of reciprocal assistance, before agreeing to help foreign authorities.

2. Conducting Investigations Pursuant to 28 U.S.C. § 1782

The US SAFE WEB Act would also give the FTC the ability to use an existing federal statute – 28 U.S.C. § 1782 – to gather evidence for a foreign law enforcement agency in certain categories of cases. As with the provision allowing the FTC to use a CID on behalf of foreign law enforcers, this provision would allow the FTC to provide assistance in foreign actions benefitting U.S. consumers.

Under Section 1782, a district court may order, pursuant to a letter rogatory or on application of any interested party, that a person within the district give his testimony or statement or produce a document or thing for use in a foreign or international proceeding.[12] To execute a Section 1782 request, a district court may appoint a person in the U.S. to obtain the requested evidence. The Department of Justice ("DOJ") routinely uses this provision in executing letters rogatory and requests under criminal mutual legal assistance treaties, with Assistant U.S. Attorneys filing an action to provide assistance to the foreign interested party.[13] Courts can also appoint private attorneys to seek assistance under this provision.[14] Section 1782 is frequently used when foreign proceedings are already in progress, and the foreign litigant needs to obtain evidence from the U.S. expeditiously.

Section 1782 would enable the FTC to assist a foreign agency, permitting the FTC to go directly into court to take testimony or seek the production of documents or things, rather than employing an investigatory tool like a CID. The FTC's ability to use this procedure would advance the twin aims of Section 1782 – providing efficient assistance to participants in international litigation and encouraging foreign countries by example to provide similar assistance to U.S. litigants.[15]

The following scenario illustrates the benefit of this procedure. Assume, for example, that the Danish consumer protection agency has launched legal proceedings against a Danish business that is harming U.S. and Danish consumers by selling phony domain names over the Internet. During the trial, the Danish agency learns that a former employee of the Danish business who has critical information about the scheme lives in the United States. The Danish agency needs to obtain testimony from the former employee quickly. It asks the FTC for help. With the authority to use Section 1782, the FTC could file an action in the federal district court of the jurisdiction where the former employee is located, and obtain the employee's testimony for use in the Danish trial.

3. International Agreements

In some cases, foreign law requires that the FTC enter into a formal international agreement to effect reciprocal investigative and evidentiary cooperation. For example, Part III of Canada's Competition Act requires a formal international agreement as a prerequisite for certain types of cooperation by the FTC's counterpart agency, Competition Bureau Canada.[16] In

addition, the European Union recently adopted a Regulation that envisions international agreements with non-European countries for cooperation on consumer protection matters.[17] If the FTC had the authority to enter into such an agreement, it could increase cooperation with consumer protection authorities in 25 individual European countries with a single agreement.

The FTC does not have the authority to enter into formal binding international agreements either in its own name or in the name of the United States on consumer protection cooperation without the US SAFE WEB Act.[18] The proposed US SAFE WEB Act would allow the FTC, subject to prior approval and ongoing oversight by the Department of State, to negotiate and conclude international agreements of this type.[19]

C. Obtaining More Information from Foreign Sources

US SAFE WEB Act § 6(b): Protects information provided by foreign enforcers from public disclosure if confidentiality is a condition of providing it. **Similar to** longstanding SEC and CFTC authority. **Needed** because, without it, some foreign law enforcers will not give the FTC information needed to halt fraud, deception, spam, and spyware.

The US SAFE WEB Act would enable the FTC to obtain information it would not otherwise receive from foreign entities. It would do so by protecting the confidentiality of the following materials received by the FTC: (1) material obtained from a foreign government agency, if the foreign agency requests confidential treatment as a condition of providing the material, (2) consumer complaints obtained from any other foreign source, if that source requests confidential treatment as a condition of providing the complaints, and (3) consumer complaints submitted to a joint project such as *econsumer.gov*.[20]

The first part of this provision is modeled on SEC[21] and CFTC[22] provisions in this area. It addresses the concern expressed by some foreign government agencies that materials they share with the FTC might be publicly disclosed in response to an inquiry under the Freedom of Information Act ("FOIA").[23] This concern is reflected in certain foreign laws, such as Canada's Competition Act[24] and the European Union's enforcement cooperation regulation.[25] Under these laws, neither the Canadian nor the European consumer protection agencies are permitted to share certain information with the FTC unless the FTC can keep such information confidential, even after an investigation is over. Currently, we cannot guarantee such confidentiality; therefore, we

cannot obtain some extremely valuable information.

For example, assume that both the Swedish consumer protection agency and the FTC are investigating a Florida-based spammer. The Swedish agency is subject to the European regulation described above. The Swedish agency has taken the testimony of a former partner of the Florida-based spammer, and the FTC requests a copy of the testimony to generate leads in its investigation. If this information had been submitted by a U.S. state agency, the FTC Act would have provided full protection. However, the FTC Act's confidentiality provisions currently would not fully protect such information obtained from a foreign agency.[26] Accordingly, the Swedish authority will not share it.

This provision would have a tremendous salutary effect on the FTC's efforts to protect U.S. consumers. It would allow the FTC to obtain much more information from its most active partner against fraud - Canada.

The US SAFE WEB Act also would exempt from public disclosure consumer complaints that the FTC receives from foreign government and private sector sources. The FTC seeks ongoing submissions of consumer complaints for its flagship consumer fraud complaint database, *Consumer Sentinel*, which is used by over 1,300 law enforcement agencies in the United States, Canada, and Australia via a secure website. The ability to guarantee confidentiality of consumer complaints from foreign sources would help the FTC to obtain a greater number of consumer complaints to add to the *Consumer Sentinel* database. This would in turn help the FTC and other U.S. law enforcement agencies with access to *Consumer Sentinel* to act on the basis of more complete information and target law enforcement efforts in areas in which there has been the most harm.

Finally, the proposed US SAFE WEB Act would exempt from public disclosure consumer complaint information submitted to joint consumer complaint projects such as the international website *econsumer.gov*.[27] Some foreign agencies have been unwilling to join *econsumer.gov* due to concerns about disclosure of information contained in consumer complaints. Indeed, several of these agencies have told the FTC that, under their laws, consumer complaints are required to be kept confidential and are not subject to public disclosure. The fact that complaints entered into *econsumer.gov* could be subject to disclosure under FOIA has deterred some foreign agencies from joining the project.[28]

Thus, the US SAFE WEB Act exempts from public disclosure the above-mentioned categories of information to facilitate the gathering of more information to fight cross-border fraud and deception. The exemption would not authorize the Commission to withhold such information from Congress or prevent the Commission from complying with a court order in an action commenced by the United States or the Commission.

II. Improving the FTC's Ability to Obtain Information Supporting Cross-Border Cases

A. Protecting the Confidentiality of FTC Investigations

> US SAFE WEB Act § 7: Safeguards FTC investigations in a defined range of cases by (1) generally protecting recipients of Commission CIDs from possible liability for keeping those CIDs confidential; (2) authorizing the Commission to seek a court order in appropriate cases to preclude notice by the CID recipient to the investigative target for a limited time; and (3) tailoring the mechanisms available to the Commission to seek delay of notification currently required by the Right to Financial Privacy Act ("RFPA") or the Electronic Communications Privacy Act ("ECPA"), to better fit FTC cases. **Similar to** longstanding RFPA, ECPA, and securities law provisions. **Needed to** prevent notice to investigative targets that are likely to destroy evidence or to move assets offshore or otherwise conceal them, precluding redress to consumer victims.

When the FTC investigates violations of the FTC Act and the other laws it enforces, it often relies on CIDs to third parties, such as banks, credit card companies, payment processors, commercial mail receiving agencies, ISPs, and domain registrars, to obtain information about identified targets. The success of FTC action often depends on keeping investigations and, in particular, CIDs, confidential. If targets are given notice that the FTC is investigating them, they can disappear (including changing their online identities) and/or conceal assets or transfer assets or records abroad, beyond the reach of U.S. courts.

Several third parties have informed the Commission that they would provide notice to a target before providing information to the FTC in response to a CID.[29] Motivations for providing notice include institutional policies and liability concerns, even when federal law does not require such a notice. The Commission has no means in most instances of preventing recipients of CIDs from providing notice to the targets. In such circumstances, the Commission often

decides not to issue the CID because it would tip off the target to the investigation.[30]

In addition, the FTC itself is required to notify investigative targets when it serves CIDs seeking certain information from certain financial institutions or ISPs. Under the Right to Financial Privacy Act ("RFPA"), in certain cases, the FTC must notify individuals and certain small partnerships if it seeks to obtain information about them from financial institutions.[31] Similarly, under the Electronic Communications Privacy Act ("ECPA"), the FTC is required to give notice to a subscriber or customer of an ISP when it seeks to obtain information about certain electronic communications.[32] Both of these laws authorize, in limited circumstances, delay for a limited period both of the agency's notice and of any notice by the recipient of the CID.[33] Circumstances justifying a delay include those where there is a likelihood that the target of the investigation will, upon notice, disappear, intimidate witnesses, destroy evidence, or otherwise seriously jeopardize an investigation. It is not clear, however, that the FTC can avoid notice when the target is likely to transfer assets or records outside the United States. Based on negative experiences, the FTC does not seek information from third parties when notice requirements would be triggered.

The US SAFE WEB Act would address these issues in three ways. It would (1) generally exempt recipients of Commission CIDs from possible liability for keeping those CIDs confidential;[34] (2) authorize the Commission to seek a court order in appropriate cases to delay notice by the recipient of the CID to the investigative target for a limited time;[35] and (3) tailor the mechanisms available to the Commission in specified appropriate instances to seek delay of notification required by RFPA or ECPA, to better fit FTC cases.

First, the US SAFE WEB Act would provide an exemption from liability for recipients of Commission CIDs for keeping the CIDs confidential. At a workshop on cross-border fraud that the Commission held in 2003, industry representatives expressed concerns about liability for failure to notify a customer about the existence of a government subpoena, even when RFPA notice requirements do not apply. As one financial regulator stated in this context, "banks do get sued and they are a little bit gun shy."[36] The US SAFE WEB Act exemption from liability for keeping a CID confidential could go a long way to alleviate this concern. This exemption is similar to 31 U.S.C. § 5318(g),[37] which exempts financial institutions from liability for sharing information about money laundering with the Department of Treasury.

Second, when neither the RFPA nor the ECPA notice provisions apply, the US SAFE WEB Act would authorize the Commission to seek a court order, in strictly limited circumstances and for a strictly limited period of time, to delay notice by the recipient of a CID to the investigative target. The circumstances under which courts could order delay of notice are modeled on a provision of the Securities Exchange Act.[38]

Finally, the US SAFE WEB Act would tailor the mechanism available for the FTC to seek court-ordered delay of notice to targets by the FTC under RFPA and ECPA. There are two main reasons for this proposed provision. First, the circumstances under which delayed notice is permitted under RFPA and ECPA are not specifically tailored to address situations the FTC routinely faces, such as where notice is likely to cause investigative targets to conceal or send offshore assets obtained through fraud. The US SAFE WEB Act would authorize court orders for the agency to postpone providing notice in the same circumstances described above, modeled on existing Securities Exchange Act language.[39] Second, it is not clear that the authority of FTC attorneys to directly litigate enforcement actions, set forth in Section 16 of the FTC Act, includes seeking court orders for delay under RFPA and ECPA. The US SAFE WEB Act would ensure that the FTC could seek such orders directly.

In proposing these changes, the FTC recognizes that there is a balance to be struck between the government's need for information and privacy interests. The FTC believes that the US SAFE WEB Act is consistent with that balance. In every instance in which the FTC seeks to compel confidentiality, it would be required to seek a court order and provide specific justification for that order. And even if the court issues such an order, it only applies for a limited period of time.

B. Protecting Certain Entities Reporting Suspected Violations of Law

US SAFE WEB Act § 8: Protects a limited category of appropriate entities from liability for voluntary disclosures to the FTC about suspected fraud or deception, or about recovery of assets for consumer redress. **Similar to** longstanding protections for financial institutions making disclosures of suspected wrongdoing to federal agencies. **Needed because** liability concerns discourage third-party businesses from alerting the FTC to suspected law violations or recoverable assets.

The US SAFE WEB Act exempts certain specified entities from liability for voluntarily sharing information with the FTC. The US SAFE WEB Act provision in this area is modeled generally upon 31 U.S.C. § 5318(g), a "safe harbor" provision for financial institutions that report possible illegal activities to government agencies.[40]

Private sector representatives have expressed reservations about voluntarily sharing information with the FTC.[41] The US SAFE WEB Act would alleviate these concerns by exempting certain third parties from liability for sharing information with the FTC, thereby improving the FTC's ability to gather information to fight spam, spyware, fraud, deception, and other illegal practices.

There are several types of information that the private sector could share with the FTC that would be useful in cross-border investigations. For example, although some entities share consumer complaints with the FTC and other law enforcement agencies through the *Consumer Sentinel* database, other entities are reluctant to share such complaints. ISPs receive numerous complaints about deceptive spam and other fraudulent activities, but some ISPs view ECPA as not permitting them to share these complaints with the FTC. The proposed amendment would clarify that ISPs can share complaints with the FTC without fear of incurring liability under ECPA.[42]

Another category of information that would be particularly useful for the FTC in investigating fraud and deception would be chargeback information from card network operators.[43] Allowing law enforcement to have access to information about which merchants have unusually high chargeback rates would enable the law enforcers to target resources more systematically.[44]

The FTC's need for these types of information is particularly evident in its cross-border investigations. If the FTC is investigating a foreign target, as a practical matter it has no way of obtaining such information because it typically does not have the power to enforce a CID that it sends abroad.[45] In many instances, while the perpetrators of fraud and deception are abroad, U.S.-based third parties might unknowingly be assisting such perpetrators by providing certain infrastructure services in the United States. If these third parties could inform the FTC when they suspect fraudulent or deceptive activity, this could go a long way to helping the FTC in its cross-border cases.

C. Allowing Information Sharing with Federal Financial and Market Regulators

US SAFE WEB Act § 10: Adds the FTC to RFPA's list of financial and market regulators allowed to readily share appropriate information. The list already includes the SEC and the CFTC. **Needed to** help the FTC track proceeds of fraud, deception, or other illegal practices sent through U.S. banks to foreign jurisdictions, so they can be recovered and returned to consumer victims.

The FTC has not been included in an exemption provided in RFPA that allows federal financial and market regulators to share financial records, examination reports, or appropriate supervisory or other information.[46] Such interagency information sharing with the FTC currently only extends to certain FTC antitrust functions, through specific authorization in federal financial services statutes.[47]

In the cross-border context, interagency information sharing with financial regulators would be particularly helpful in tracking assets for consumer redress. In particular, such information sharing would be useful where fraud proceeds are sent through U.S. banking establishments to foreign jurisdictions and may have been the subject of a Suspicious Activity Report concerning money laundering.

For example, suppose the FTC brings an action against the perpetrators of a fraudulent Internet service scheme that charged millions of dollars, without authorization, to consumer credit card accounts. The fraud operators obtain the consumers' credit card information from a federally regulated bank. In connection with the Internet service scheme, many millions of dollars are sent through multiple U.S. multinational banks to offshore jurisdictions, in part to make it difficult for the FTC to collect those assets for distribution as redress to consumers. In some of the jurisdictions, the same fraud perpetrators are charged with money-laundering offenses concerning those funds transfers. If the FTC had access to Suspicious Activity Reports filed in connection with entities which the FTC is investigating, it would make FTC efforts at tracking assets more efficient and less costly. It also would increase the likelihood of distributing redress funds to victims of cross-border fraud schemes rather than allowing fraudsters to spend their ill-gotten gains.

III. Improving the FTC's Ability to Take Effective Action in Cross-Border Cases

A. Enhancing Cooperation Between the FTC and DOJ in Foreign Litigation

US SAFE WEB Act § 5: Permits the FTC to cooperate with DOJ in using additional staff and financial resources for foreign litigation of FTC matters. **Needed because,** without additional resources to freeze foreign assets and enforce U.S. court judgments abroad, fraudsters targeting U.S. consumers can more readily use the border as a shield against law enforcement.

The US SAFE WEB Act would support the Commission's efforts to obtain repatriation of assets for consumer redress in two specific ways. First, it would authorize the FTC to use appropriated funds to reimburse the Department of Justice ("DOJ") for expenses incurred in foreign litigation of FTC matters. Second, it would authorize the Commission, with the concurrence of the Attorney General, to designate Commission attorneys to assist the Attorney General in connection with such litigation.

The pursuit of assets in foreign jurisdictions is vital to the Commission's goal of providing consumers with redress in cross-border matters. The Commission increasingly is litigating many cases against foreign defendants who have foreign assets and domestic defendants who have transferred their assets abroad to place them beyond the reach of U.S. courts. This presents significant obstacles to the Commission's ability to obtain the proceeds of fraud and deception for eventual restitution to defrauded consumers.

Currently, DOJ pursues litigation outside the United States on behalf of the FTC by hiring foreign attorneys to represent the FTC in foreign courts and supervising the foreign litigation.[48] The Commission has had considerable success in pursuing foreign assets through DOJ. But DOJ's resources to assist the FTC are limited, and the FTC's cross-border caseload is growing.

The FTC's mission would be materially advanced if the Commission could use its legal talent and appropriated funds to partner more closely with DOJ in pursuing litigation in foreign courts. The US SAFE WEB Act would allow the Commission to use appropriated funds toward retaining foreign counsel to bring preliminary asset freeze actions and post-judgment foreign recognition and enforcement proceedings, significantly increasing the resources available to

recover money on behalf of fraud victims.

In addition to authorizing this use of appropriated funds, the US SAFE WEB Act would provide for the FTC to be more directly involved in cases filed in foreign courts, leveraging the expertise of its staff litigators. FTC attorneys are intimately familiar with the facts of FTC cases and the manner in which fraudsters use the border to shield themselves from law enforcement. With DOJ guidance, FTC attorneys could supplement the existing limited staff resources that DOJ has to supervise foreign counsel in such cases. Indeed, there is precedent for such a mechanism: Congress has enacted legislation explicitly permitting DOJ to receive details of personnel and funds from other federal agencies.[49]

B. Confirming the FTC's Remedial Authority in Cross-Border Cases

US SAFE WEB Act § 3: Expressly confirms: 1) the FTC's authority to redress harm in the United States caused by foreign wrongdoers and harm abroad caused by U.S. wrongdoers; and 2) the availability in cross-border cases of all remedies available to the FTC, including restitution. **Needed to** avoid spurious challenges to jurisdiction in FTC cases and to encourage the full range of remedies for U.S. consumer victims in foreign courts.

The proposed US SAFE WEB Act contains a provision confirming 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 spam, spyware, telemarketing fraud, and other law violations. Specifically, the legislation provides that the Commission may challenge unlawful and deceptive practices that cause or are likely to cause reasonably foreseeable injury within the United States, or that involve material conduct occurring within the United States. It further confirms the Commission's ability to obtain remedies, including restitution, for domestic and foreign consumers injured by such practices. These criteria are similar to those developed by federal courts defining the SEC's authority to address securities and investment fraud involving foreign nations and actors.[50]

The Commission's authority to act in cases involving foreign actors or unlawful conduct occurring beyond U.S. borders has a long history. Under the Act, "unfair or deceptive acts or practices in or affecting commerce" are declared unlawful,[51] and "commerce" is defined to include

commerce with foreign nations.[52] The federal courts have construed this language as authorizing the Commission to act in cross-border matters.[53] Indeed, the FTC Act has been applied repeatedly to schemes originating abroad that have harmed U.S. consumers.[54] The FTC's authority to prosecute such cases prevents foreign defendants who cause concrete harms occurring in the United States from escaping liability.

The FTC Act has also been applied to schemes originating in the United States that have targeted foreign consumers.[55] The FTC's ability to act in such scenarios deters fraud operators from using the United States as a haven from which they can develop and then export fraudulent schemes.[56] It also protects U.S. businesses from dishonest competitors and aids the FTC in obtaining reciprocal cooperation from its foreign law enforcement partners.

Despite this history and the strong reasons for permitting the FTC to exercise its authority in cross-border cases, legal decisions in a few non-FTC cases have led to a lack of clarity in this area of the law.[57] As a result, 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.[58] The Commission expects that such challenges will continue to mount as the Commission brings more and more cases that have cross-border elements. Congressional action would confirm the FTC's authority to take action in this area.

By 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. Clarifying the ability of the FTC to provide redress to foreign consumers would also encourage foreign agencies to provide similar redress to U.S. consumers.

C. Clarifying FTC Authority to Make Criminal Referrals

US SAFE WEB Act § 4(b) (adding FTC Act § 6(k)): Expressly authorizes the FTC to make criminal referrals for prosecution when violations of FTC law also violate U.S. criminal laws. **Similar to** existing FTC authority to provide information to criminal authorities, a narrow express criminal referral provision in the FTC Act, and an SEC provision. **Needed because** foreign agencies that address consumer fraud and deception as a criminal (not civil) law enforcement issue would be more willing to share information if the FTC has express authority to share information with criminal authorities.

The proposed US SAFE WEB Act contains a provision expressly authorizing the FTC to make criminal referrals of violations of unfair or deceptive acts or practices under the FTC Act to the DOJ.[59] It further provides that the Commission shall endeavor to ensure that material it obtains from foreign law enforcement agencies may be used for the purpose of investigation, prosecution, or prevention of violations of United States criminal laws. The US SAFE WEB Act's section is modeled on the SEC's broad criminal referral provision.[60]

Such an express criminal referral provision will help the FTC obtain information from foreign criminal law enforcement agencies that prosecute consumer fraud through their criminal law systems. These agencies are sometimes reluctant or unwilling to share substantial information or work closely with an agency like the FTC, a civil agency that may have no exact counterpart in their country. The US SAFE WEB Act's express criminal referral provision will highlight the role the FTC plays in the U.S. dual civil/criminal enforcement system, and thereby address concerns of foreign criminal enforcement agencies about sharing information with a civil enforcement agency that might have no counterpart in their country.

The proposed change would also make it more likely that the FTC would fall within the ambit of proposed Mutual Legal Assistance Treaties ("MLATs") that have been written with some role for regulatory agencies that have criminal referral powers. Traditionally, MLATs facilitate the exchange of information between law enforcement agencies with criminal authority. As a civil law enforcement agency, the FTC therefore is generally unable to use the MLAT mechanism to obtain information needed to advance its investigation of or litigation against a civil target. Some more recent MLATs, however, contemplate cooperation between civil and criminal enforcement agencies. For example, the MLAT between the United States and Luxembourg explicitly states that the U.S. Central Authority may make requests under the MLAT on behalf of

"prosecutors, investigators with criminal law enforcement jurisdiction, and agencies or entities with specific statutory or regulatory authority to refer matters for criminal prosecution"(emphasis added).[61] Other MLATs contain similar language.[62]

The FTC's role in developing cases that ultimately become criminal matters, particularly those involving fraudulent or deceptive conduct, already is substantial. Indeed, FTC investigations and judicial proceedings frequently result in subsequent criminal prosecutions.[63] And in 2003, the FTC established a Criminal Liaison Unit to build on its successful cooperation with criminal law enforcement agencies.[64] Thus, a Congressional grant of explicit authority to make criminal referrals in appropriate cases involving unfair or deceptive practices under Section 5 of the FTC Act would not change materially the actual scope of the Commission's legal powers. It would, however, send a clear signal to foreign criminal law enforcement agencies about the appropriateness of sharing information with the FTC.

IV. Strengthening the FTC's Cooperation and Relationship with Foreign Authorities

A. Providing for Foreign Staff Exchange Programs

US SAFE WEB Act § 9: Provides for foreign staff exchange arrangements between the FTC and foreign government authorities, and permits the FTC to accept reimbursement for its costs in these arrangements. **Needed to** improve international law enforcement cooperation in cross-border matters.

The proposed US SAFE WEB Act authorizes the FTC to conduct staff exchange programs, under which employees of foreign government agencies could be detailed to work at the FTC on specific cases and investigations, and FTC employees could be detailed to work for foreign agencies. The US SAFE WEB Act provision is analogous to other Congressional authorizations facilitating staff exchanges.[65]

Staff exchanges would help the FTC, and in turn, U.S. consumers, by improving the skills of FTC employees and foreign law enforcers in combating fraud and deception and improving international law enforcement networks.[66] To have a fully successful staff exchange program,

foreign government officials detailed to the FTC should be able to work on appropriate cases and investigations, and in such matters to have access to non-public case files.[67] Allowing foreign employees to work on FTC cases and investigations and have access to confidential material would help those employees learn about FTC investigative techniques and later adopt those techniques in their agency investigations. They could also provide significant help investigating joint cases involving evidence or witnesses located in their country. For example, a foreign employee from a Canadian agency could provide significant help in an FTC investigation into telemarketing fraud originating in Canada.

The US SAFE WEB Act's provision on staff exchanges is necessary to provide consent pursuant to the Emoluments Clause of the Constitution, which prohibits, without the consent of Congress, (1) foreign government officials from being put in a position of "trust" by the United States, or (2) those holding a position of "profit" or "trust" in the United States from being employed by a foreign government.[68] Providing a foreign government employee who is detailed to the FTC to assist with an investigation with access to confidential FTC information arguably puts that person in a position of "trust" under the Emoluments Clause. Similarly, the Emoluments Clause would preclude an FTC employee from being employed by a foreign government. An explicit Congressional authorization of staff exchanges between the FTC and foreign government agencies would obviate any concerns that such exchanges may violate the Emoluments Clause and provide additional resources to the FTC in cross-border spam, spyware, and telemarketing fraud cases.

B. Authorizing Expenditure of Funds on Joint Projects

US SAFE WEB Act § 4(b) (adding FTC Act § 6(l), 4(c)): Authorizes the FTC to expend appropriated funds, not to exceed $100,000 annually, toward operating expenses and other costs of cooperative cross-border law enforcement projects and bilateral and multilateral meetings. **Similar to** SEC authority. **Needed to** allow the FTC to help support valuable international cooperative organizations and projects such as the website or consumer education programs of the International Consumer Protection and Enforcement Network (ICPEN) that foster the FTC's mission.

The US SAFE WEB Act would allow the Commission to expend a limited amount of funds for operating expenses and other costs of bilateral and multilateral cooperative law enforcement organizations, including ICPEN, the International Competition Network, Mexico-

U.S.-Canada Health Fraud Task Force, Project Emptor, Toronto Strategic Partnership, and additional task forces with law enforcement agencies in other Canadian provinces. It would also allow the Commission to expend a limited amount of funds for certain expenses arising from consultations hosted by the Commission with foreign counterparts. Currently, expenditure of funds on joint projects and bilateral and multilateral meetings may be prohibited by various appropriation statutes, unless there is a specific statutory authorization for such expenditure.[69] The US SAFE WEB Act provision is analogous to specific statutory authority provided to the SEC.[70] The US SAFE WEB Act provision caps the amount for such expenditures at $100,000. Although the amount of such contemplated expenditures is small, it can yield significant dividends because the work of these partnerships leverages the resources of all agencies working on consumer protection issues.

This provision would assist U.S. consumers by allowing the FTC to target more resources where they are needed. For example, at a meeting of one of the U.S.-Canada task forces to combat cross-border telemarketing fraud, participants decided that it would be useful to have a car to use for surveillance of boiler rooms where fraudulent telemarketers had set up their operations. The FTC could not contribute to purchasing a used car for this purpose, and therefore, sufficient funds were not available. The US SAFE WEB Act would remedy this problem and others like it.

C. Leveraging the FTC's Resources Through Reimbursement, Gift Acceptance, and Voluntary and Uncompensated Services

US SAFE WEB Act § 11: Authorizes the FTC to accept reimbursement for providing assistance to law enforcement agencies in the U.S. or abroad, and to accept gifts and voluntary services in aid of the agency's mission and consistent with ethical constraints. **Similar to** the authority of numerous regulatory agencies, including the SEC and the CFTC, and of the FTC and DOJ in the antitrust context, to accept reimbursements from foreign counterparts. **Needed to** assure that in appropriate circumstances a foreign agency bears the costs of FTC efforts on their behalf, and to enable the FTC to employ volunteers as our Canadian counterparts have done successfully for years.

The US SAFE WEB Act gives the FTC authority to accept reimbursement from other law enforcement agencies, including its counterparts abroad, for providing investigation, litigation, or other program assistance and for joint projects. This provision is modeled on existing provisions

in the Securities Exchange Act, the Commodity Exchange Act, and other statutes.[71]

The authority to accept reimbursement for providing investigative and case assistance will promote the efficient use of FTC resources, allowing the FTC to provide the assistance to generate goodwill and reciprocity without expending its own funds. For example, if an Asian consumer protection authority is investigating a weight-loss scam, in which a deceptive advertiser targeted primarily Asian consumers, and learns that the target has fled to the United States, it may ask the FTC to hire a private investigator and to work with him or her to locate the target. The Asian authority may need such assistance because of time differences and language problems. The FTC's provision of this assistance at no cost to it could lead to reciprocal help from Asian authorities.

The ability to seek reimbursement would also benefit joint projects. For example, the FTC wants to modify the *econsumer.gov* website to accept a broader range of languages and provide a broader range of features. Other authorities have expressed an interest in contributing financially toward improvements to the site, but the FTC currently cannot accept such payment.

Currently, the FTC cannot receive reimbursements under the Miscellaneous Receipts Act, which requires all funds received by the U.S. government to be deposited into the U.S. Treasury, "except as provided by another law."[72] The US SAFE WEB Act would provide the necessary statutory authorization.

The US SAFE WEB Act also includes a provision authorizing the FTC to accept gifts and voluntary and uncompensated services in aid of the agency's mission, consistent with ethical constraints. Numerous agencies, including law enforcement and regulatory agencies, have this authority.[73] The FTC continues to believe that authority to accept gifts and voluntary uncompensated services would be helpful, both in the domestic and cross-border contexts. For example, this authority would enable the FTC to accept voluntary contributions from foreign governments for joint projects such as *econsumer.gov*. It would also enable the FTC to employ volunteers, as its Canadian counterparts have done successfully for years.[74]

Endnotes

1. This legislation is largely identical to S. 1234, 108th Cong., 2d Sess. (2004), and to H.R. 3143, 108th Cong., 2d Sess. (2004), *available, in a report of the Committee on the Judiciary, at* http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr635p2&dbname=cp108&. *See also* S. Rep. No. 127, 108th Cong., 1st Sess. (2003), 2003 WL 22022750 (Leg.Hist.), *available at* http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr127&dbname=cp108&; H.R. Rep. No. 635(I), 108th Cong., 2d Sess.(2004), 2004 WL 1835122 (Leg.Hist.), *available at* *http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr635p1&dbname=cp108&*; H.R. Rep. No. 635(II), 108th Cong., 2d Sess.(2004), 2004 WL 2623198 (Leg.Hist.), *available at* http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr635p2&dbname=cp108&.

2. Such information may only be shared with foreign law enforcement with the consent of the submitter. *See* 15 U.S.C. § 57b-2(b)(3)(c)); 16 C.F.R. § 4.10(d); *see also* 15 U.S.C. §§ 46(f), 57b-2(b)(6); 16 C.F.R. § 4.11(c)).

3. The proposed US SAFE WEB Act would allow the FTC to share information with a foreign agency that is investigating violations of foreign laws prohibiting fraudulent or deceptive practices or other practices substantially similar to practices prohibited by consumer protection laws administered by the FTC or, with the approval of the Attorney General, other foreign criminal laws that are encompassed in an applicable MLAT. It would also allow the FTC to share information in order to gain assistance in its own matters from a foreign law enforcement agency.

4. 15 U.S.C. § 78x(c).

5. 7 U.S.C. § 12(e).

6. 12 U.S.C. § 3109.

7. This document discusses scenarios setting forth examples of the types of problems the Commission faces in its cases and investigations. These scenarios are based on real cases and investigations. In some instances, we have combined facts from more than one case or investigation and/or changed country names to preserve the confidentiality of investigative information.

8. The proposed US SAFE WEB Act would allow the FTC to provide investigative assistance when a foreign agency is investigating violations of laws prohibiting fraudulent or deceptive practices or other practices substantially similar to practices prohibited by consumer protection laws administered by the FTC.

9. 15 U.S.C. § 57b-1.

10. This obstacle to investigative cooperation is separate from the obstacles to information sharing discussed above. Not only does the Commission need the authority to share with foreign law enforcers information obtained in its own investigations regardless of whether the submitter of information consents to the sharing, it also needs the authority to issue CIDs to gather information in cases it is not otherwise investigating. In certain cases, even if U.S. consumers are involved, as in this example, there may be no independent reason for opening an FTC investigation because there may be no effective relief to pursue through an FTC action given the circumstances of a particular case. However, through the strengthened investigative cooperation recommended here, the Commission could play a role in addressing the harmful practices at issue.

11. 15 U.S.C. § 78u(a)(2); 7 U.S.C. § 16(f); 12 U.S.C. § 1818(v)(2).

12. 28 U.S.C. § 1782.

13. *See, e.g., In re Commissioner's Subpoenas*, 325 F.3d 1287 (11th Cir. 2003); *In re Letter of Request from the Crown Prosecution Serv. of the United Kingdom*, 870 F.2d 686 (D.C. Cir. 1989); *In re Letter of Request from the Boras Dist. Court, Sweden*, 153 F.R.D. 31 (E.D.N.Y. 1994); *In re Letter of Request From the Gov't of France*, 139 F.R.D. 588 (S.D.N.Y. 1991).

14. *See, e.g., In re Letter of Request for Judicial Assistance from Tribunal Civil de Port-au-Prince, Republic of Haiti*, 669 F. Supp. 403 (S.D. Fla. 1987).

15. *See* S. Rep. No. 1580, 88th Cong., 2d Sess. 2 (1964), *reprinted in* 1964 U.S.C.C.A.N. 3782, 3783 (expressing goal of "providing equitable and efficacious procedures for the benefit of tribunals and litigants involved in litigation with international aspects," and thereby "invit[ing] foreign countries similarly to adjust their procedures"); *see also In re Malev Hungarian Airlines*, 964 F.2d 97, 100 (2d Cir. 1992).

16. Competition Act [Canada], Part III: Mutual Legal Assistance, § 30 et seq., *available at* http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=1304&lg=e

17. Commission Regulation 2006/2004/EC, 2004 J.O. (L 364) 1, *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_364/l_36420041209en00010011.pdf.

18. The FTC may sign informal, non-binding memoranda of understanding, and has already done so. Unfortunately, these memoranda of understanding do not rise to the level of formality to satisfy some foreign legal prerequisites to consumer protection information sharing and cooperation.

19. The criteria for international agreements are set forth in statutes and regulations. *See* 1 U.S.C. §§ 112a - 112b; 22 C.F.R. 181.1 *et seq.*

20. *See* www.econsumer.gov. The *econsumer.gov* website is 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.

21. 15 U.S.C. § 78x(d); *see also* H.R. Rep. No. 240, 101st Cong., 1st Sess. 2, 11-12, 23-25 (1989), *reprinted in* 1990 U.S.C.C.A.N. 3888, 3889, 3898-99, 3910-12.

22. 7 U.S.C. § 12(a)(1); *see also* H.R. Conf. Rep, No. 978, 102nd Cong., 2nd Sess.70-71 (1992), *reprinted in* 1992 U.S.C.C.A.N.3202-03; S. Rep. No. 22, 102nd Cong., 1st Sess. 71 (1991) *reprinted in* 1992 U.S.C.C.A.N. 3173.

23. 5 U.S.C. § 552. FOIA would not protect information from public disclosure if there were no ongoing FTC investigation into the company that is the subject of the information. Nor would it protect from public disclosure information about an investigative target after the investigation has closed.

24. Without this provision, the Competition Act would bar execution of a civil mutual legal assistance treaty, needed to allow Competition Bureau Canada to help the FTC on matters it is not investigating itself. Competition Act [Canada], Part III: Mutual Legal Assistance, § 30 *et seq.*, *available at* http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=1304&lg=e#partIII.

25. The European Union regulation states that information shared between member countries to enforce consumer protection laws may only be used for the purpose of "ensuring compliance with the laws that protect consumers' interests" and that "[i]nformation exchanged . . . should be subject to the strictest guarantees of confidentiality . . . ." *See* Commission Regulation, *supra* note 17, at 7, 2. Discussions with European Commission representatives have revealed that, under these provisions, European authorities would similarly not share information with the FTC unless the FTC guarantees the confidentiality of such information. We cannot do so sufficiently under current law.

26. *See* 15 U.S.C. §§ 57b-2(b), 57b-2(f). Since, as a practical matter, the Commission cannot enforce compulsory process against a foreign entity, the complete protection from disclosure contained in 15 U.S.C. § 57b-2(f) likewise does not apply.

27. *See supra* note 20.

28. The exemption from disclosure described in the previous paragraph would apply to complaints collected by foreign government agencies and private sector entities and shared with the FTC subject to a request for confidential treatment. The exemption described in this paragraph would apply to consumer complaints submitted directly by consumers to a joint database that the FTC sponsors with foreign consumer protection agencies.

29. *See* Transcript of FTC February 2003 public workshop on Public/Private Partnerships to Combat Cross-Border Fraud [hereinafter "Cross-Border Fraud Tr."], Flynn (FTC) (Feb. 19) at 128-29 and Wenger (FTC) (Feb. 20) at 89-90, *available at* http://www.ftc.gov/bcp/workshops/crossborder/index.html.

30. *See id.,* Flynn (FTC) (Feb. 19) at 128-29 and Wenger (FTC) (Feb. 20) at 89-90.

31. 12 U.S.C. § 3405.

32. 18 U.S.C. § 2703(b). This provision covers situations in which the FTC seeks to obtain information from electronic communications services about "the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days" or, generally, from a provider of remote computing services about the contents of an electronic communication held or maintained on behalf of a subscriber or customer or for the purpose of providing storage or computer processing services to subscribers or customers.

33. 12 U.S.C. § 3409; 18 U.S.C. § 2705.

34. This provision would not apply when the notice or delayed notice provisions of RFPA and ECPA are triggered.

35. As with the first provision, this provision would not apply when the notice or delayed notice provisions of RFPA and ECPA are triggered.

36. Cross-Border Fraud Tr., *supra* note 29, Schultz (Feb. 19) at 137.

37. This section provides that "[a]ny financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority, and any director, officer, employee, or agent of such institution who makes, or requires another to make any such disclosure, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." 31 U.S.C. § 5318(g)(3)(A).

38. 15 U.S.C. § 78u(h).

39. *Id.*

40. The exemption from liability under 31 U.S.C. § 5318(g) is broad. It "applies whether the financial institution makes a required or volunteered report . . .; whether the report is made to federal, state, or local authorities . . .; whether the reported activity eventually turns out to be legal or illegal . . .; and whether the report is made with or without a good faith investigation . . . ." *Gregory v. Bank One, Ind., NA,* 200 F. Supp. 2d 1000, 1002-03 (S. D. Ind. 2002) (internal citations omitted).

41. Cross-Border Fraud Tr., *supra* note 29, Beales (Feb. 20) at 252-53. As a representative of a domain registrar suggested, the goal is "to try and get the whole public/private partnership together such that fraud can be prevented at source and registrars aren't exposed to liability . . . ." *Id.*, Kane (Feb. 20) at 222-23. Another panelist related an anecdote about how a bank would not cooperate with the FBI in a particular matter unless it was given a hold harmless clause. *Id.*, Schultz (Feb. 19) at 145.

42. Although ECPA generally prohibits voluntary sharing of information by ISPs about their customers, there is an exception that permits ISPs to disclose electronic communications with the consent of the intended recipient of a communication. 18 U.S.C. § 2702(b)(3). If a customer sends a complaint to an ISP, the ISP is the "intended recipient" and presumably could consent to share that complaint with the FTC. Thus, the proposed provision would not expand the categories of information ISPs can share under ECPA; it would merely clarify that ECPA does not prohibit an ISP from sharing complaints that it receives.

43. A chargeback is a mechanism "whereby if there is a problem with a merchant and a customer has not made a particular transaction, but the merchant has tried to put it through the system, there is a mechanism for charging that back so that the customer is not responsible for it." Cross-Border Fraud Tr. *supra* note 29, MacCarthy (Feb. 19) at 175.

44. *Id.*, Burg (Feb. 19) at 189-90.

45. 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 refused 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.-Austl., 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.

46. *See, e.g.,* 12 U.S.C. § 1828b.

47. 12 U.S.C. § 1828b; *see also* 12 U.S.C. § 1849(b)(1); 15 U.S.C. § 41 note.

48. The FTC possesses independent litigating authority to represent itself by its own attorneys in several categories of cases including suits under Section 13(b) of the FTC Act, the Commission's principal enforcement vehicle for consumer protection matters. *See* 15 U.S.C. §§ 56, 57(b). Despite this broad Congressional grant of independent litigating authority, which could be interpreted as giving the FTC the authority to conduct litigation in foreign and international tribunals independent of DOJ, the FTC believes that the appropriate legislative course is to amend the FTC Act to (1) authorize the Commission to expend appropriated funds on the retention of foreign counsel and other litigation expenses in foreign courts and (2) include provisions increasing the role of FTC attorneys in litigation brought on the FTC's behalf by DOJ.

49. 28 U.S.C. § 543. This provision authorizes attorneys from other government agencies to work as Special Assistant U.S. Attorneys, whereas the proposed provision under the US SAFE WEB Act would allow FTC attorneys to work with DOJ's Office of Foreign Litigation, which is responsible for U.S. government litigation abroad.

50. *See, e.g., North-South Finance Co. v. Al-Turki,* 100 F.3d 1046, 1051-52 (2d Cir. 1996) (summarizing, in RICO case, analysis used by courts in considering the applicability of U.S. securities laws to transnational securities frauds).

51. 15 U.S.C. § 45(a)(1).

52. 15 U.S.C. § 44.

53. The seminal case, decided in 1944, is *Branch v. FTC*, 141 F.2d 31 (7th Cir. 1944). There, the Commission enjoined a U.S. citizen from making false and misleading representations about his correspondence school to consumers in Latin America. On appeal, the United States Court of Appeals for the Seventh Circuit affirmed the injunction, holding that "[i]t is true that much of the objectionable activity occurred in Latin America; however, it was conceived, initiated, concocted, and launched on its way in the United States. That the persons deceived were all in Latin America is of no consequence." *Id.* at 34-35.

54. *See, e.g., FTC. v. Cleverlink Trading Ltd., et al.*, Case No. 05 C 2889 (N.D. Ill., filed May 16, 2005), *available at* http://www.ftc.gov/opa/2005/05/housewives.htm; *FTC and The People of the State of California v. Opt-In Global Inc., d/b/a Vision Media Ltd.*, C 05 1502 SC (N.D. Cal., filed Apr. 5, 2005), *available at* http://www.ftc.gov/opa/2005/04/optin.htm; *FTC v. 9125-8954 Quebec Inc., a corporation d/b/a Global Mgmt. Solutions, et al.*, Civil Action No. CV-005-0265 (W.D. Wash., filed Feb. 15, 2005), *available at* http://www.ftc.gov/opa/2005/03/abs.htm; *FTC v. Sun Ray Trading, Inc. et al.*, Civil Action No.: 05-20402 CIV-Seitz (S.D. Fla., filed Feb. 10, 2005), *available at* http://www.ftc.gov/opa/2005/02/bizoppflop.htm; *FTC v. Sobonito Investments Ltd.*, Civ. A. No. 05C 580 (N.D. Ill., filed Feb. 1, 2005), *available at* http://www.ftc.gov/opa/2005/02/sobonito.htm; *FTC v. Millenium Mktg.*, Civl A. No.: 04C 7238e (N.D. Ill., filed Nov. 9, 2004), *available at http://www.ftc.gov/opa/2004/11/millineum.htm; FTC v. Global Web Promotions Pty Ltd. et al.,* Civ. A. No., 04C 3022 (N.D. Ill., filed Apr. 28, 2004), *available at* http://www.ftc.gov/opa/2004/04/040429canspam.htm; *FTC v. No. 1025798 Ontario, Inc., a corporation d/b/a Beauty Visions Worldwide, Kingstown Assocs. Ltd. et al.*, Civ. A. No. 03 CV 0910 (W.D.N.Y., filed Dec. 3, 2003), *available at* http://www.ftc.gov/opa/2003/12/weightlosscases.htm; *FTC v. Brian D. Westby et al.*, Civ. A. No. 03 C 2540 (N.D. Ill., filed Apr. 17, 2003), available at http://www.ftc.gov/opa/2003/04/westby.htm; *FTC v. CSCT, Inc. et al.*, Civ. A. No. 03 C 00880 (N.D. Ill., filed Feb. 6, 2003), *available at* http://www.ftc.gov/opa/2003/02/csct.htm; *FTC v. Carlton Press, Inc. et al.*, Civ. A. No. 03-CV-0226-RLC (S.D.N.Y., filed Jan. 10, 2003); *available at* http://www.ftc.gov/opa/2003/01/idpfinal.htm; *FTC v. Dr. Clark Research Ass'n et al.*, Civ. A. No. 1:03CV0054 (N.D. Ohio, filed Jan. 8, 2003), *available at* http://www.ftc.gov/opa/2003/01/drclark.htm; *FTC v. Mountain View Systems, Ltd. et al.*, Civ. A. No. 1:03-CV-OOO21-RMC (D.D.C., filed Jan. 7, 2003), *available at* http://www.ftc.gov/opa/2003/01/idpfinal.htm; *FTC v. First Capital Consumers Group et al.*, No.: 02C 7456 (N.D. Ill., Oct. 17, 2002), *available at* http://www.ftc.gov/opa/2002/10/firstcap.htm; *FTC v. Hudson Berkely Corp. et al.*, No. CV-S-02-0649-PMP-RJJ (D. Nev. filed May 7, 2002), *available at* http://www.ftc.gov/opa/2002/05/projectabsurd.htm; *FTC v. TLD Network Ltd. et al.*, No.: 02-C-1475(N.D. Ill., filed Feb. 28, 2002), *available at* http://www.ftc.gov/opa/2002/03/tld.htm; *FTC v. Opco Int'l Agencies et al.*, No.: C01-2053R (W.D. Wa., filed Feb. 21, 2001), *available at* http://www.ftc.gov/opa/2001/02/opco.htm ; *FTC v. Growth Plus Int'l*, No. 00C 07886 (N.D. Ill, filed Dec. 18, 2000), *available at* http://www.ftc.gov/opa/2000/12/gains2.htm; *FTC v. Verity Int'l*, No.: 00-CIV-7422 (LAK) (S.D.N.Y., filed Oct. 2, 2000), *available at* http://www.ftc.gov/opa/2000/10/verity.htm; *FTC v. Pereira*, Civ. Action No. 99 Civ. 562 (RJD) (E.D. Va., filed Jan. 29, 1999), *available at* http://www.ftc.gov/opa/1999/09/atariz.htm; *FTC v. Win USA Serv., Ltd.,* C.98-1614Z (W.D. Wash., filed Nov. 3, 1998), *available at* http://www.ftc.gov/os/2001/02/winfinord.pdf; *FTC v. Pacific Rim Pools Int'l,* C97-1748 (W.D. Wash., Nov. 7, 1997), *available at* http://www.ftc.gov/opa/1999/01/poolswoof.htm; *FTC v. Tracker Corp.*, Civ. Action No. 97-CV-2654 (N.D. Ga., filed Sept. 11, 1997), *available at* http://www.ftc.gov/opa/1997/09/tracker.htm; *FTC v. 9013-0980 Quebec Inc., ("Incentive International")*, 1996 U.S. Dist. LEXIS 18,897 (N.D. Ohio, filed Aug. 13, 1996), *available at* http://www.ftc.gov/opa/1996/07/jackpot.htm; *FTC v. Ideal Credit Referral Serv. Ltd.,* No. C96-0874R (W.D. Wash., filed June 5, 1996), *available at* http://www.ftc.gov/opa/1997/04/ideal.htm.

55. *See, e.g., FTC v. Skybiz.com, Inc.*, No. 1-CV-396-EA(X) (N.D. Okla., filed May 30, 2001), *available at* http://www.ftc.gov/opa/2001/06/sky.htm; *FTC v. Fortuna Alliance*, Civ. No. C96 799M (W.D. Wash., filed May 23, 1996, *available at* http://www.ftc.gov/opa/1996/05/fortuna.htm.

56. This rationale has been expressed by the federal courts in the securities law context. *See IIT v. Vencap, Ltd.,* 519 F.2d 1001, 1017 (2d Cir.1975) (permitting suits involving material conduct occurring in the United States on the theory that Congress did not want "to allow the United States to be used as a base for manufacturing fraudulent security devices for export, even when these are peddled only to foreigners.").

57. *See, e.g., E.E.O.C.v. Arabian Am. Oil Co.*, 499 U.S. 244, 264 (1991); *Nieman v. Dryclean U.S.A. Franchise Co.*, 178 F.3d 1126 (11th Cir. 1999).

58. For example, in the FTC's *Skybiz* litigation, *supra* note 55, the defendants – primarily U.S.-based individuals and companies – challenged the district court's issuance of a preliminary injunction under the FTC Act to halt the defendants' marketing of a deceptive pyramid scheme to U.S. and foreign consumers. *See FTC v. SkyBiz.com, Inc.*, 1-CV-396-EA(X) (N.D.Okla.) (Brs. of Defs. dated Jan. 17, 2002 and Jan. 25, 2002 and Reply Br. of Pl. Federal Trade Comm'n dated Feb. 1, 2002) (on file with FTC). The district court and the Tenth Circuit found that the FTC Act did apply to the defendants' conduct, including the transactions with foreign consumers. *See FTC v. Skybiz.Com, Inc.*, 57 Fed. Appx. 374, 2003 WL 202438, at *2 (10th Cir. Jan. 30, 2003) (table decision; text available in Westlaw). *See also Matter of Telebrands Corp.*, 2004 WL 817051, Docket No. 9313 (Order Denying Cmpl. Counsel's Mot. to Comp. Production of Docs. and Answers to Interrogs.) (FTC, Feb. 25, 2004), *vacated in relevant part by* Order Denying Mot. to Reconsider or To Certify for Interlocutory App. (FTC, Mar. 25, 2004).

59. The FTC Act already contains a limited criminal referral provision; however, that provision is focused on those portions of the Act that carry criminal penalties and not on the types of cross-border spam, spyware, and telemarketing fraud that are the focus of this legislation. *See* 15 U.S.C. § 56(b). Congress also has granted the Commission authority to disclose nonpublic material to federal and state law enforcement agencies, including criminal agencies, where the agency certifies that the material will be maintained in confidence and used only for official law enforcement purposes. 15 U.S.C. § 57b-2(b)(6); 15 U.S.C. § 46(f).

60. 15 U.S.C. § 77t(b); s*ee also* 15 U.S.C. § 78u(d).

61. Treaty on Mutual Legal Assistance in Criminal Matters, Mar. 13, 1997, U.S.-Lux., S. Treaty Doc. No. 105-11.

62. *See, e.g.,* Treaty on Mutual Legal Assistance in Criminal Matters, Jan. 16, 1998, U.S.-Lith., S. Treaty Doc. No. 105-41; Treaty on Mutual Legal Assistance in Criminal Matters, Feb. 4, 1998, U.S.-Czech. Rep., S. Treaty Doc. No. 105-47.

63. From April 2, 2004 to April 1, 2005, there were 52 separate matters where formal criminal litigation was ongoing or initiated against FTC defendants or their close associates, or where the FTC provided significant assistance to criminal authorities.

64. The FTC has established a special Criminal Liaison Unit to expand criminal prosecution of consumer fraud. The Criminal Liaison Unit identifies enforcement agencies that may bring specific types of consumer fraud cases, educates criminal law enforcers in areas of FTC expertise, and coordinates training with criminal authorities to help the FTC prepare cases for referral and parallel prosecutions. Since 1996, dozens of FTC civil cases have resulted in concurrent or subsequent criminal prosecutions. The Criminal Liaison Unit will build on these existing FTC efforts to ensure appropriate criminal prosecution of consumer fraud.

65. *See, e.g.,* 37 U.S.C. § 908 (permitting certain members of the military to accept employment with foreign governments); 22 U.S.C. § 3622(f) (same for Panama Canal authority).

66. The types of exchanges contemplated here would not involve exchanges in highly classified or sensitive areas. Indeed, the FTC is often pursuing the same targets as its foreign counterparts, and the ability to develop joint investigations and cases while a foreign employee is detailed to the FTC would be highly beneficial. The same reasoning applies in the antitrust area, and therefore, we recommend that this provision cover staff exchanges on both the competition and consumer protection sides of the FTC's mission.

67. The FTC has engaged in limited staff exchange programs under which it has hosted visitors for a few weeks at a time, set up meetings for the visitors, and worked with the visitors on non-case related joint projects. These exchanges, particularly with visitors from the Australian Competition and Consumer Commission, Danish Consumer Ombudsman's Office, Spanish Data Protection Authority, and Japan Fair Trade Commission have improved our communication and information exchanges with these agencies. However, these visits could have been even more productive if the visitors were permitted to assist FTC staff on particular cases.

68. U.S. Const. art. I, § 9, cl. 8.

69. *See* Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, Division H, Title VI, § 610, 118 Stat. 2809, *3274; 31 U.S.C. § 1345; General Accounting Office, Office of the General Counsel, *Principles of Federal Appropriations Law* (2 ed.) at 4-84 to 4-86, 4-88 to 92, 4-100 to 4-103.

70. *See* Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, Division B, Title V, 118 Stat. 2809, *2910.

71. 15 U.S.C. § 78d(f); 7 U.S.C. § 16(f)(3). Among the other agencies with reimbursement acceptance authority are the FCC, 47 U.S.C. § 154, and the FTC (with respect to antitrust), 15 U.S.C. § 6212.

72. 31 U.S.C. § 3302(b).

73. Agencies with this authority include: the Federal Communications Commission, 47 U.S.C. § 154; the Consumer Product Safety Commission, 15 U.S.C. § 2076; the Federal Reserve Board, 12 C.F.R. § 264b; the National Credit Union Administration, 12 U.S.C. § 1772a; and the National Transportation Safety Board, 49 U.S.C. § 1113.

74. For example, PhoneBusters, Canada's national fraud call center operated by the Ontario Provincial Police and Royal Canadian Mounted Police, employs volunteers in its SeniorBusters program. SeniorBusters presently consists of more than 60 volunteer members over the age of 50. These volunteer members come from diverse backgrounds and help SeniorBusters in its attempt to reduce the level of fraudulent telemarketing against seniors. SeniorBusters contact family members, local police agencies, elder abuse committees, and provide seniors with the necessary tools to effectively fight this crime.