Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

18-Oct-2004

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/CP/ICCP/SPAM(2004)4
Unclassified

Task Force on Spam

SPAM RELATED LAW ENFORCEMENT ACTIONS

The following tables, prepared by the Secretariat, are intended to provide the OECD Task Force on Spam with information about actions taken against spammers by public enforcement agencies. In particular, the tables illustrate various forms of abuse committed through email and SMS spam, the variety of actors involved in the enforcement of anti-spam laws and the range of remedies and sanctions available to them.

Task Force members are invited to discuss and decide what further action should be taken in this area. The Secretariat requests Task Force Members to verify, and if necessary correct, the information provided on cases in their countries and to provide any new or missing information. The Secretariat would like to make the tables of cases available on its Spam webite.

Anne Carblanc, Tel: + 33 145 24 93 34, anne.carblanc@oecd.org
Michael Donohue, Tel: + 33 1 45 24 14 79, michael.donohue@oecd.org
Jack Radisch, Tel: + 33 1 45 24 76 86, jack.radisch@oecd.org

JT00171978

English - Or. English

NOTE BY THE SECRETARIAT

The attached tables were prepared by the Secretariat based on research it conducted using publicly available documents and sources. The tables are an illustrative, not exhaustive, list of actions taken by public enforcement agencies against email and SMS spammers. The variety of illegal activities includes: phishing attacks, fraudulent or deceptive marketing of goods and services, advance fee and securities fraud, denial of service attacks, sending unsolicited commercial email, using a false return address or misleading subject line, and failure to respect opt-out requirements or requests.

Table I comprises 11 cases, each brought under a specific anti-spam law.

Table II comprises 84 cases brought under laws not specifically enacted to address the problem of spam.

- 54 cases were brought by Consumer Protection Authorities.
- 17 cases were brought by Criminal Prosecutors.
- 11 cases were brought by Communications Regulators.
- 6 cases were brought by Data Protection Authorities.
- 6 cases were brought by Securities Regulators.
- 1 case was brought by an Advertising Standards Authority

Table I: CASES BROUGHT UNDER A SPECIFIC ANTI-SPAM LAW

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
Denmark	Danish National Consumer Agency vs. Aircom Erhverv ApS www.juriscom.net/actu/visu.php?ID=419	The Consumer Protection Ombudsman brought suit against a Danish telecom company that had sent over 15, 000 unsolicited commercial e-mails to private consumers and companies.	Law on marketing practices	Fine of DKK 400,000 (approx. USD 68,000)	The defendant argued that the law did not apply since the e-mails had been sent from outside Denmark. The court ruled that the marketing law applies to foreign source spam, as long as the sponsoring company is Danish and the recipient e-mail address is based in Denmark, and left open the possibility that it could even apply to non-Danish sponsoring companies.	Unknown
	Danish National Consumer Agency vs. Fonn Danmark www.siliconvalley.com/mld/siliconvalley/5762085.htm	After receiving 50 complaints, the Consumer Protection Ombudsman brought suit against a Danish software company that had sent 156 unsolicited commercial e-mails.	Law on marketing practices	The Copenhagen Maritime and Commercial Court in Copenhagen fined Fonn DKK 13,000 (approximately U.S. $2,200).	Unknown	Unknown
Japan	MPHPT vs. Remain Inc. www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news031113_1.html http://www.soumu.go.jp/s-news/2003/031113_2.html	The MPHPT (Telecommunications Authority) issued an order of compliance measures against a company providing dating services based in Nakano-ku, Tokyo, which had sent mobile spam to mobile phones. The order requires the company to alert recipients that the messages are unsolicited and to provide a valid opt-out email address.	Law on Regulation of Transmission of Specified Electronic Mail	Unknown	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
Japan	MPHPT v. SIS World www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news040416_3.html www.soumu.go.jp/s-news/2004/040416_2.html	The MPHPT issued an order for compliance measures against a company which had sent mobile spam without providing the name of the company, announcing that the message was unsolicited and not providing an email address to opt-out of further messages.	Law on Regulation of Transmission of Specified Electronic Mail	Unknown	Unknown	Unknown
United States	FTC vs. Creaghan www.ftc.gov/os/caselist/0423085/0423085.htm	The FTC received 40,000 consumer complaints about spam linked to the defendant and his web sites that sell bogus anti-ageing products. The defendant operated the web sites through aliases and foreign addresses, and disguised the source of the e-mails by forging return addresses in the "from" fields and sending them through open proxies.	CAN-SPAM Act and Section 5, FTC Act	A federal judge issued a temporary restraining order prohibiting spamming, false product claims, and freezing the defendant's assets. The merits of the case have not yet been litigated.	The defendant resides in Florida, and identifies his business as being located in Canada, Sweden and Switzerland. The products are sold on web sites with domain names registered to individuals in China. Proceeds from sales are wired to a Latvian bank.	Unknown
	FTC vs. Phoenix Avatar LLC www.ftc.gov/os/caselist/0423084/040429phoenixavatarmemo.pdf www.usdoj.gov/opa/pr/2004/April/04_crm_281.htm	Consumers forwarded over 490 000 e-mails to the FTC regarding the defendant's fraudulent weight loss patches and body enlargement pills. The e-mails used forged "from" addresses, and failed to provide clear and conspicuous opportunity to opt-out from receiving future messages or a valid physical address.	CAN-SPAM Act	A federal judge initially issued a temporary restraining order prohibiting spamming, false product claims, and freezing the defendant's assets. Criminal charges are pending.	Unknown	The Department of Justice, which is bringing a separate criminal complaint against the defendants, ISPs and the US Postal Service provided investigation assistance by following the paper trail left in registering for web sites through which the products were sold

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Bryant and Bryant www.ftc.gov/os/caselist/0423125/041005gbacmp.pdf	Defendants sent deceptive spam that claimed recipients could make substantial income through a business opportunity with a false "money back guarantee" by stuffing envelopes at home. The defendants charged a $25 registration fee and $25 for a kit which did not contain letters to fill, rather two pages of instructions and a CD ROM which explained how to perpetuate the same scam. The emails contained spoofed header information, and false return information.	CAN-SPAM Act, 5 FTC Act and 45(a) of the Telemarketing Sales Rule.	A federal judge issued an asset freeze and a temporary restraining order prohibiting further sales and shipment of the products. Proceedings in civil court seeking a permanent injunction and consumer redress are pending.	Unknown	Unknown
	FTC vs. Global Web Productions www.ftc.gov/os/caselist/0423086/040428globalwebmemosupporting.pdf	Consumers forwarded nearly 400,000 e-mails to the FTC regarding the defendant's fraudulent weight loss patch and anti-aging spray.	CAN-SPAM Act	A federal judge issued a temporary restraining order prohibiting further sales and shipment of the products.	The defendants reside in Australia and New Zealand, and Global Web is based in Australia. The web sites through which sales are conducted routinely change registry between Japan, Malaysia, Hong Kong and Singapore.	The case was brought with the assistance of the Australian Competition and Consumer Commission and the New Zealand Commerce Commission.

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	United Stats of American vs. Nicholas Tombros www.securityfocus.com/news/9606	Defendant drove around a suburb and used a laptop and wi-fi antenna to locate unsecured residential internet access points, which he then used to send thousands of messages advertising pornography sites. Tombros was charged with a provision under the CANSPAM Act which prohibits breaking into someone else's computer to send spam.	CAN-SPAM Act	Defendant entered a plea agreement and will be sentenced in December 2004. A first-time violator face up to one year in federal stir for a small-time operation-- three years if he or she meets one of several minimum standards of bad behaviour, like leading a spam gang of at least three people, sending over 2 500 messages in one day, or using 10 or more falsely-registered domain names	Unknown	Unknown
	United Stats of American vs. Smathers and Dunaway http://newpaper.asia1.com.sg/top/story/0,4136,66784-1096646340,00.html	The Defendants are charged with conspiracy to steal data of 30 million AOL customers, and some 92 million e-mail addresses. Dunaway purchased the list of email addresses from Smathers, an AOL employee, and sold it for US$52,000 to spammers. Dunaway later bought an updated version of the list for US$100,000, and resold it again.	CAN-SPAM Act	The defendants each face a maximum sentence of five years in prison and a fine of US$250,000, or twice the gain or loss from the offence.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	United States vs. Chung, Sadek, Lin and Lin (Phoenix Avatar LLC) www.usdoj.gov/opa/pr/2004/April/04_crm_281.htm	Four men were charged with sending hundreds of thousands of commercial email messages advertising diet patches and other devices, while using false and fraudulent headers to hide their identities. The criminal complaint alleges that the defendants were responsible for devising a scheme to defraud others by selling these medical devices via the U.S. mail by means of false and fraudulent representations.	CAN-SPAM Act and Mail Fraud Statute	Pending. The CAN-SPAM Act carries penalties of up to three or five years' imprisonment. Violations of the mail fraud statute carry a penalty of up to 20 years' imprisonment.	Unknown	The FTC, which is bringing a separate civil suit against the defendants, ISPs and the U.S. Postal Service provided investigation assistance by following the paper trail left in registering for web sites through which the products were sold

Table II: CASES BROUGHT UNDER GENERAL LAW

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
Australia	ASIC vs. Hourmouzis www.internetnews.com/bus-news/article.php/499241	The Australian Securities and Investments Commission charged the defendant with interruption of the lawful use of file server computers, and making a statement that was false or misleading and likely to induce the purchase of securities. The defendant sent more than 4 million e-mails to discussion boards, claiming certain stock would rise to US $3 or more. Subsequently the price doubled on a trading volume that was more than 10 times the previous month's average, and the defendant sold his shares on the first trading day after the transmissions, making a profit of US $17,000.	Securities regulations	Defendant plead guilty and was sentenced to two years' imprisonment. The U.S. Securities and Exchange Commission instituted its own proceedings against the man and obtained a judgment ordering that he disgorge ill-gotten profits of US $15,000	The Australian resident sent e-mails to addresses in the United States, Australia and other parts of the world, after purchasing 65,000 shares in Rentech through a stock broking firm in Canada.	Unknown
	People vs. Marinellis www.news.com.au/common/story_page/0,4057,7726290%255E15306,00.html	The defendant operated a "419" advance fee scam, sending e-mail with messages to convince people that they were entitled to claim millions of dollars through lottery winnings, an inheritance or a business opportunity if they first sent off money for "expenses". The defendant collected a total of $5 million from victims worldwide.	17 charges including five criminal counts of conspiring with others to cheat and defraud.	Pending	The defendant claims to be the Australian contact for an organisation with 220 operatives acting globally.	Unknown
Canada	Case name unknown http://p2pnet.net/story/1546	A juvenile suspected of hacking into thousands of computers was charged with mischief and fraudulent use of a computer by infecting computers with a "Trojan" virus that forces them to send thousands of e-mails at once with the aim to make the recipient system crash.	Criminal law	Pending	Unknown.	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
China	People vs. Jianquan and Wenqui http://latelinenews.com/ll/english/1311289.shtml	The defendants used phone text messages to swindle money from subscribers by telling them that they had won lottery prizes. The recipients were told they could claim their prize by sending lottery tax payments to designated bank accounts.	Criminal law	A court in the province of Fujan sentenced one man to eight years imprisonment for obtaining $16,000. The second man was sentenced to four years for illegal earnings of $6,000.	Unknown.	Unknown
France	Prosecutor of the Republic (TGI du Mans) vs. L www.legalis.net/jnet/decisions/diffamation/tgi_mans_071103.pdf	A former employee of a pharmaceutical company spoofed the sender address in 700,000 unsolicited emails he sent to harass his former employer. The resulting saturation of the message inbox constituted a trespass upon the company's information system.	Criminal law [Penal Code 462-2 and3].	The Tribunal de Grande Instance of Mans sentenced the defendant to a 10 month suspended jail sentence and two years probation.	Unknown	Unknown
	Prosecutor of the Republic (TGI de Paris) vs. M.R.G.V. www.juriscom.net/jpt/visu.php?ID=533	The defendant acquired a CD-ROM of 50,000 e-mail addresses and used them to send spam containing a link to a pornographic site. One recipient filed a complaint with the prosecutor.	Criminal law [Penal Code Article 226-16].	The defendant was found guilty of automatic processing of personal information without prior notification to the proper authority (the CNIL), and fined 3,000 Euro. However, the court acquitted the defendant of the charge that he had unlawfully collected personal information, citing the fact that mere possession of a CD –ROM containing personal data does not constitute collection.	Unknown	Unknown
	Prosecutor of the Republic (TGI de Draguignian) vs. Dinant No weblink available	A man was convicted of blocking the functioning of an automated information system, and the unfair collection of personal information by using a program designed to capture e-mail addresses from a service provider. The defendant disrupted the servers of Wanadoo by making 23 million individual attacks to copy e-mail addresses.	Criminal law [Penal Code 25-78-17, 226-18-1 and 226-31]	Unknown	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
France	CNIL vs. Alliance Bureaucratic Service www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-075a.pdf	The CNIL received 650 notices from email users referring to unsolicited commercial email that they had received from Alliance Bureaucratic Services. ABS is accused of having used "robot mail" to collect the recipient's email addresses, a tool which it sells. Such tools are illegal under French data protection law. Further, some of the recipients complained that there was no opt-out option in the emails that they received. Finally, the company should have notified the CNIL in advance that it would use the email addresses for the purpose of direct marketing.	Criminal law [Penal Code Article 226-16, 18].	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings.	Unknown	Unknown
	CNIL vs. Suniles www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-078a.pdf	The CNIL received 170 notices from email users referring to unsolicited commercial email that they had received from SUNILES. SUNILES is accused of having used "robot mail" to collect email addresses of the recipients, and not providing an option to opt-out of receiving future emails. Further SINALES did not notify the CNIL in advance that it would send email for the purpose of direct marketing	Criminal law [Penal Code Article 226-16, 18].	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings	Unknown	Unknown
	CNIL vs. (John Doe-company sending the emails "Le Top 50 du X") www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-079a.pdf	The CNIL received 1000 notices from email users referring to unsolicited emails that they had received from an unidentifiable source promoting pornographic websites. The internet users claimed to have never had previous contact with the websites in question. The unidentified source is accused of having used "robot mail" to collect email addresses of the recipients, and not providing an option to opt-out of receiving future emails. Further the company did not notify the CNIL in advance that it would send email for the purpose of direct marketing.	Criminal law [Penal Code Article 226-16, 18].	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to initiate criminal proceedings.	Unknown	Unknown
	CNIL vs. BV Communication http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-076a.pdf	The CNIL received 260 notices from email users referring to unsolicited commercial emails that they had received from BV Communications. The internet users claimed to have never had previous contact with the company in question. BV Communication is accused of having used "robot mail" to collect email addresses of the recipients, and not providing an option to opt-out of receiving future emails. Further the company did not notify the CNIL in advance that it would send email for the purpose of direct marketing.	Criminal law [Penal Code Article 226-16, 18].	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to file criminal charges.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
France	CNIL vs. GreatMeds.com www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-077a.pdf	The CNIL received around 500 notices from email users referring to unsolicited commercial emails that they had received from GreatMeds.com. The emails received by users contained various text and links permitting recipients to navigate to the company's website through which it sells various medications online. The internet users claimed to have never had previous contact with the company in question. GreatMeds.com is accused of having used "robot mail" to collect email addresses of the recipients, and not providing an opportunity to opt-out of receiving future emails.	Criminal law [Penal Code Article 226-18].	Pending. The CNIL forwarded an official complaint to the Public Prosecutor for it to decide, in its discretion, whether to file criminal charges.	GreatMeds.com is apparently a company located in the United States.	Unknown
Italy	Garante vs. unknown company www.legalday.co.uk/lexnex/evershed03/November/e80281103.htm	The Italian Data Protection Authority (Garante) reported a graphic arts business to the Italian criminal court, on grounds that it had continued to send spam even after the Garante issued a "data processing block". In addition the company failed to comply with an order requesting information regarding the origin of the personal data used in the spam, and the name of the person responsible for its processing treatment. Some recipients of the spam had complained to the Garante, claiming that the company had sent them advertising and promotional communications without having the necessary "informed" consent from them.	The new Data Protection Code enacted in June 2003 provides for criminal sanctions if personal data is processed without complying with the obligation to inform consumers and obtain their consent.	The representative of the company was fined 15,000 Euro for failure to comply with the DPA request. Criminal proceedings are pending and could potentially lead to up to 3 years' imprisonment.	Unknown	Unknown
Japan	METI v. Access Control www.meti.go.jp/policy/consumer/release/remain.pdf	The Ministry of Economy, Trade and Industry ordered Access Control to cease violations resulting from its failure to identify itself in unsolicited email and not providing an email address for the purpose of opting out from future unsolicited email.	Specified Commercial Transactions Law	No further action taken. Continued violation would be referred to criminal authorities	None	None
Korea 25 separate cases	Case name unknown times.hankooki.com/lpage/biz/200402/kt2004020919282811860.htm	The Korean Fair Trade Commission responded to 212 complaints of spam by ordering 25 spammers to correct their unlawful online advertising practices and issuing fines. The company receiving the heaviest fine arbitrarily sent spam even after consumers had opted-out. The FTC director general in charge of the consumer protection bureau announced that they were reviewing business suspension and heavier fines as possible future measures.	E-Commerce Consumer Protection Law	Fines ranged from 1 to 7 million won ($5,800), and two adult phone services were fined 5 million won each for sending SMS spam.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
Nether-lands	Case name unknown www.dmeurope.com/default.asp?ArticleID=2428	The Dutch Ministry of Justice brought charges of a "Nigerian 419 scam" e-mail fraud in response to a complaint filed by a Dutch cable operator and ISP.	Criminal	The Amsterdam district court acquitted six of thirteen alleged e-mail scammers, due to lack of sufficient evidence; ruling that the discovery of the suspects at locations from where spam was being distributed was insufficient grounds for a conviction. The Dutch public prosecutor is appealing the decision. The prosecution had collected evidence at the time and place of arrest including: illegal internet-connections, spamming software, mobile handsets, Nigerian scam letter-templates and even piles of names and addresses. However, the prosecution failed to prove convincingly that the suspects used the confiscated equipment to commit the alleged crimes at the locations in question.	Victims of the e-mail scam resided in Japan and the U.S. The defendants did not appear at the first trial and are thought to have fled the country, raising the question of the practical value of an appeal. The Dutch police confirmed ties between the defendants and drug smugglers in the Dutch Antilles.	Unknown
Russia	Case name unknown http://english.pravda.ru/main/18/90/361/13170_spam.html	Cell phone operator "Uralsky GSM" complained to the police that more than 15,000 cell phone owners were receiving unsolicited SMS. Upon investigation police confiscated the computer containing software for sending the SMS-messages, which the defendant had created himself. He was charged with creating software to perform denial of service attacks, and copying personal information	Unknown	The defendant pled guilty, was put on probation for one year and required to pay fine of 3,000 roubles ($100).	Unknown	Unknown
Switzer-land	Case name unknown www.edsb.ch/d/doku/empfehlungen/spam_neu.pdf	Upon complaints by recipients of unsolicited commercial e-mail, the Federal Data Protection Commissioner (SDPC) sent notice to a man sending spam to businesses and private individuals to provide information in his possession about the recipients and to delete it. The SDPC gave him thirty days to comply with the request, or the matter would be referred to a prosecutor	Art. 29-3 of the Federal Data Protection Act	Pending	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United Kingdom	Case name unknown software.silicon.com/security/0,39024655,39122143,00.htm	A man who had been fired for failing to complete his time-sheet retaliated by launching a denial of service attack against his former employer (UK insurers Domestic & General). The five-million mail attack brought down the corporate website and cost an estimated £18,000 in lost business. The defendant admitted using a spam tool which he downloaded from the internet.	Criminal	The defendant faces six months in prison or a fine of up to £5,000.	Unknown	Scotland Yard's computer crime unit identified him and had him arrested.
	ICSTIS vs. BW Telecom www.icstis.org.uk/icstis2002/default.asp?node=74&month=2	The Independent Committee for the Supervision of Standards of Telephone Information Services ("ICSTIS"), the industry-funded regulatory body for all premium rate charged telecommunications services, fined BW Telecom £75,000 for sending unsolicited e-mails that indirectly promoted a premium rate adult Internet site to random e-mail addresses with no apparent attempt made to prevent them from being sent to children. The email contained peak-rate dialler software which disconnected users from their ISP before reconnecting them to a service that charged them £1.50 a minute for Net access.	ICSTIS Code of Practice	ICSTIS barred access to service for a period of 12 months and instructed BW Telecom to offer redress to all 240 complainants	U.S. company based in New York	Unknown
6 separate cases	ICSTIS vs. Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd and Quartel Ltd //www.theregister.co.uk/2004/05/24/text_fine_icstis/	Responding to thousands of complaints, ICSTIS-the premium rate watchdog, levied fines on six companies for sending text spam, making unsolicited phone calls and using automated calling equipment to leave "missed calls" on mobile phones, tempting punters to phone back on premium-rate phone numbers costing up to £1.50 a minute. The regulator found that these companies deliberately tried to con people into calling premium-rate numbers to claim prizes that didn't exist or didn't match what was promised	ICSTIS Code of Practice	Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd and Quartel Ltd were ordered to pay fines of £75,000 each, and redress to those affected, and barred from operating in the UK	The six companies are based overseas and had been operating through the same UK based agent, Smile Telecom of Bury	The Department of Trade and Industry, communications regulator Ofcom and the police have also been called in to investigate the links between those involved
	ICSTIS vs. ACME Marketing http://www.icstis.org.uk/icstis2002/default.asp?node=74&id=2	ICSTIS acted on complaints from the public about receiving SMS spam that informed recipients that they could claim either a holiday or £5,000 and invited them to call a premium rate number to find out how. The text message failed to state call costs and company identity/contact details, while none of the recipients had consented to receiving it Monitoring showed that callers could only actually claim the holiday and would be entered into a draw to win a £5,000 prize	ICSTIS Code of Practice	ACME Marketing was fined £3,000 and access to the service was barred for a period of six months. They were also instructed to offer redress to all complainants	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United Kingdom	Advertising Standards Authority vs. C Fry http://www.asa.org.uk/adjudications/show_adjudication.asp?adjudication_id=37209&from_index=by_media&dates_of_adjudications_id=546	ASA upheld several complaints concerning unsolicited commercial emails selling a prank CD-ROM and telephone call service. The emails contained misleading headers, were sent without the explicit consent of recipients, and claimed that they had been sent as opt-in promotions from partner companies.	Advertising Code	The ASA instructed the advertiser to ensure that in future promotional e-mails were sent only to consumers who had consented to receive them and that consumers who had given consent were given an opportunity to opt-out on each occasion. The sender claimed that he had not sent the messages, but the ASA noted that the emails appeared to have been sent either by or on behalf of the individual, and had ignored requests to show that recipients had consented to receiving the messages.	Unknown	Unknown
United States	FTC vs. Westby and Bevelander http://www.ftc.gov/opa/2003/09/fyi0357.htm	The FTC alleged that the defendants sent e-mails containing false or misleading header information, spoofed e-mail addresses and provided opt-out links that didn't function.	§5(a) of the FTC Act	Settlement bars the defendants from spoofing, using deceptive subject lines, false header information, or making false claims that they will remove consumers from e-mail lists. In addition, the defendants must give up USD112,500 in ill-gotten gains made from the alleged illegal activities [USD87,500 from Westby and USD25,000 from Bevelander]. The settlement also contains recordkeeping provisions to allow the FTC to monitor compliance.	The defendants, Westby and Bevelander, reside in Missouri and the Netherlands respectively. The businesses through which they operated, Maps Holding B.V. and PB Planning & Services B.V. have their principal places of business also in the Netherlands and are incorporated there.	Unknown.
	FTC vs. Zachary Keith Hill ; United States vs. Keith Hill www.ftc.gov/os/caselist/0323102/040322cmp0323102.pdf www.ftc.gov/os/caselist/0323102/040322pleaagree0323102.pdf	Defendant hijacked corporate logos and used deceptive spam to induce consumers into providing 473 credit card numbers and other personal financial information and then illegally purchased USD47,000 in merchandise.	§5(a) of the FTC Act and Section 521 of the Gramm-Leech-Bliley (GLB)Act, Criminal: 18 US Code, 1029 (a)(5)	Defendant settled FTC charges that his scam violated federal laws, however he was later convicted in a separate criminal proceeding initiated by the US Department of Justice and sentenced to 46 months of prison.	Unknown.	Assistance from the FBI Washington Field Office, and U.S. Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad.

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. a minor www.ftc.gov/os/2004/06/040518stipaminorbyhisparents.pdf	The minor defendant copied corporate logos and deceptive spam to conduct a classic phishing attack, conning consumers out of credit card numbers and other financial data	§5(a) of the FTC Act and Section 521 of the Gramm-Leech-Bliley (GLB)Act	Defendant settled FTC charges that his scam violated federal laws. If approved by the court, the defendant, a minor, will be barred for life from sending spam and would give up USD3,500 in ill-gotten gains.	Unknown.	Assistance from the FBI Washington Field Office, and U.S. Attorney for the Eastern District of Virginia's Computer Hacking and Intellectual Property Squad.
	FTC vs. GM Funding http://www.ftc.gov/os/caselist/dojsweep/030505gmfundstip.pdf http://www.ftc.gov/os/caselist/dojsweep/030505universalstip.pdf	Defendant conducted phishing attacks with forged e-mail headers. A phishing attack begins with an email which claims to be from a service to which the recipient belongs and might make electronic payments to such as: a bank or online retailer. The email claims that the recipient must update his personal information for this service to continue, by filling in an online form on a site which resembles the true website of the bank or retailer represented. The online form typically includes space for credit card numbers and identifying information such as social security numbers, date of birth account number and address. Once the information is sent, the defendant could use the information to transfer funds from victim's bank accounts, apply for credit cards in their names or purchase goods online.	§5(a) of the FTC Act and Section 521 of the Gramm-Leech-Bliley (GLB)Act	A settlement bans defendants from sending spam and requires them to give up USD60,500 in ill-gotten gains.	Unknown.	Coordination of efforts with other federal, state and local law enforcers.
	FTC vs. Patrick Cella et al www.ftc.gov/os/caselist/dojsweep/031119cellastipjudg.pdf www.ftc.gov/os/caselist/dojsweep/031119herrerazezulastip.pdf	The defendants used deceptive spam and Web sites to advertise that for a USD50 advance payment, consumers would receive envelopes and pamphlets. They claimed that they would pay consumers USD1 apiece for stuffing the envelopes and claimed that consumers could make USD 500 to USD 1,500 a week doing so. Some of the spam promised that consumers' payments were fully refundable. Instead of receiving envelopes and pamphlets, consumers received a booklet containing instructions on how to market the defendants' deceptive credit repair manual to other consumers. No consumers made the promised earnings, and consumers did not receive refunds.	§5(a) of the FTC Act	Settlements with the defendants permanently bar them from sending spam, from making deceptive representations, and from providing others with the means and instrumentalities to commit deception. Defendants will provide USD 7,000 for consumer redress. If the financial representations are found to be inaccurate, USD 536,412, the total of their ill-gotten gains, will be due.	Unknown.	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. K4 Global Publishing http://www.ftc.gov/os/caselist/dojsweep/031014k4globalstp.pdf	Defendants sent spam with a subject line of "Instant Internet Empires" touting the money-making potential of five pre-packaged Internet businesses. For their USD 47.77 investment, consumers received the right to reproduce the defendants' Web site and the right to try to resell its contents to other consumers. The FTC alleged that to achieve the promised earnings, consumers each would have to sell the product to 2,400 additional consumers, who would each need to sell to 2,400 additional consumers to achieve the same earnings, and so on. According to the FTC, by the third generation of the scheme, participants would need to make a total of 13,829,760,000 sales, more than twice the earth's population, for each of them to achieve the advertised earnings.	§5(a) of the FTC Act	A stipulated final judgment and order bars making false or misleading income claims, from participating in chain marketing schemes, and from providing others with the means and instrumentalities to violate federal laws. Based on financial statements provided by the defendants, USD 247,000 will be provided for consumer redress. Should the financial representations be found to be inaccurate, the total of their ill-gotten gains, USD 634,222, will become due.	Unknown	Unknown
	FTC vs. Christopher Baith, Monarrez and Verma www.ftc.gov/os/caselist/0223291/040211baithcmp0223291.pdf	Defendants sent spam promising a free Sony Playstation to lure consumers to pornographic Web sites, then redirected consumers' Internet connections through a 900-number with a significant per minute charge.	§5(a) of the FTC Act	A settlement resulted in a permanent injunction barring the defendants from sending any e-mail that misrepresents the identity of the sender or the subject of the e-mail, and a USD 10,000 fine, and USD 25,000 in ill gotten gains.	Unknown	Unknown
	FTC vs. BTV industries www.ftc.gov/os/2002/04/btvcmp.pdf	Defendants sent spam promising free gifts to consumers, who were redirected to telephone pay services when they made downloads required to claim their prize.	§5(a) of the FTC Act	A settlement resulted in a permanent injunction barring the defendants from sending any e-mail that misrepresents the identity of the sender or the subject of the e-mail, and a USD 10,000 fine, and USD 25,000 in ill gotten gains	One of the several defendants is a Spanish corporation registered in the Canary islands.	FTC worked with UK and Canary Islands
	FTC vs. Benoit www.ftc.gov/opa/1999/05/audiot10.htm	Scammers duped consumers into making costly international telephone calls in an attempt to ward off bills for merchandise they never ordered. The defendants contacted the consumers using bulk e-mail with a variety of forged addresses which prevented consumers from refuting the orders by e-mail. When consumers called the number to cancel orders for merchandise that they had never made they were automatically connected to a pay adult phone service	§5(a) of the FTC Act	U.S. telephone carriers would ordinarily bill consumers for their pay-per-call charges and forward the funds to the Dominica telephone company which in turn distributes portions of the revenue to the providers of the audiotext service. Due to time lags between billing, collection and remission payments, it would typically take about 60 days for the funds to reach the audiotext business. The court order will prevent the telephone carriers from remitting the funds now in the revenue stream and preserve the money for consumer redress.	Consumers injured by placing calls to West Indies.	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. TLD Network Ltd. et. al. www.ftc.gov/opa/2003/11/fyi0365.htm	Defendants used to spam to market the sale of non-existent domain names.	§5(a) of the FTC Act , 108(c) of the TILA, and 505(a)(7) and 522(a) of the GLB Act	Unknown	Unknown	FTC work with UK Office of Fair Trading
	FTC vs. 30 minute mortgage et al www.ftc.gov/os/2003/03/30mincmp.pdf	Defendants sent fraudulent spam advertising "3.95% 30 Year Mortgages" and described itself as a "national mortgage lender." The company urged potential customers to complete detailed online loan applications that including social security numbers, income, and assets, and assured them that transmission of the sensitive information would be protected using Secure Sockets Layer (SSL) technology	§5(a) of the FTC Act , 108(c) of the TILA, and 505(a)(7) and 522(a) of the GLB Ac	Agreed upon settlement bars the illegal practices permanently and orders the defendants to give up their ill-gotten gains. The judgments require posting USD 1 million bonds before sending unsolicited commercial e-mail. A USD 57,500 judgment against the company President has been suspended	Unknown	Unknown
6 separate but related cases	FTC vs. Larsen, Va, Lutheran, Panchero, Estenson and Boivin www.ftc.gov/opa/2002/02/eileenspam1.htm	Six defendants were charged with sending spam to consumers containing deceptive chain letters. The letters promised "USD 46,000 or more in the next 90 days," to recipients who were to send USD 5.00 in cash to each of four participants at the top of the list. In return for a USD 5.00 payment, recruits received "reports" providing instructions about how to start their own chain letter schemes and recruit tens of thousands of others via spam	Unknown	The stipulated final judgments and orders for permanent injunction bar all the defendants from promoting, marketing, advertising, offering for sale, selling, or assisting others in any chain marketing scheme	The investigation found more than 2,000 participants in the chain letter from almost 60 countries around the world.	The addresses were culled from the FTC's unsolicited commercial e-mail (UCE) database
	FTC vs. Chase Financial Funding www.ftc.gov/os/caselist/0223287/040602comp0223287.pdf	The defendants have sent spam with false and deceptive content promoting "FIXED PAYMENT" loans with rates such as 3.5 percent and 2.95 percent.	§5(a) of the FTC Act;	Court was asked to bar the defendants permanently from engaging in deceptive lending practices, and to award relief, including consumer redress and disgorgement of the defendants' ill-gotten gains.	Unknown	Unknown
	FTC vs. Clickformail.com www.ftc.gov/os/2003/10/clickformailfinalord.pdf	The defendants sent spam e-mail telling consumers they were approved and guaranteed to receive major, unsecured credit cards with credit limits up to USD 5,000 for an advance fee of USD 49.95. However, consumers who paid the fee did not receive the promised card. Instead, they allegedly received access to a set of hyperlinks to companies where consumers could apply for credit cards	§5(a) of the FTC Act	Defendants agreed to a settlement in which they are to pay USD 815,000 in consumer redress. In addition to paying redress, the settlement prohibits the defendants from making any false claims to consumers in the future.	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Universal Direct et al www.ftc.gov/os/2002/04/universaldircmp.pdf	Defendants used deceptive spam and a Web site to recruit consumers into an illegal chain letter, by sending spam that promoted "a multi-level marketing "Gifting Program " The spam claimed that participants could earn USD 10,000 in cash gifts within a few months of joining and urged consumers to recruit other participants.	§5(a) of the FTC Act	The settlement bars the defendants from promoting or selling pyramid or chain mail schemes, misrepresenting potential earnings claims, misrepresenting the legality of such schemes, failing to disclose the profits or earnings of other participants in any multilevel marketing program, and providing others with the means to make misrepresentations. Following the preliminary injunction, the defendants refunded all the money they had collected from investors in the scheme.	Unknown	Unknown
	FTC vs. Walker www.ftc.gov/os/2002/04/davidwalkercmp.pdf	Defendant used an Internet site to market products he claims cure cancer. The site claimed that the treatments, which cost between USD 2,400 and USD 5,200, make surgery, chemotherapy, and other conventional cancer treatments unnecessary. A declaration from a distinguished oncologist suggested the therapies are potentially harmful to cancer patients.	§5(a) of the FTC Act	Pending. The agency asked the court to bar the unsubstantiated claims permanently, and order consumer redress	Unknown	Unknown
	FTC vs. Cyber Data www.ftc.gov/os/2002/10/scottord.pdf	Defendant sent spam to consumers claiming that by purchasing his bulk e-mail lists, they could make money selling products and services on the Internet. Cyber Data's e-mail claimed that purchasers reasonably could expect to earn "over USD 10,000,000" by selling a USD 5 product via bulk e-mail.	§5(a) of the FTC Act	Defendant agreed to a settlement permanently barring any false, misleading, or deceptive claims about potential earnings from any bulk e-mail list, software, service, or marketing program, or any other business opportunity. Based on financial documents that the defendant provided, the settlement requires Cyber Data to pay USD 20,000 in consumer redress.	Unknown	Unknown
	U.S. vs. Internet Specialists www.usdoj.gov/usao/pae/News/Pr/2003/oct/carlson.pdf	A disgruntled baseball fan hacked into computers and from those computers launched spam e-mail attacks with long messages voicing his complaints about his favorite team's management. When launching the spam e-mails, many of the addresses on the long list were no longer current. When those e-mails arrived at their destinations, the indictment charges that they were "returned" or "bounced" back to the person who purportedly sent them – the persons whose e-mail addresses had been "spoofed" or hijacked. This caused floods of thousands of e-mails into these accounts in a very short period of time, disrupting their service.	§18 USC 1028, 1030	Unknown	Defendant gained control of a computer in Canada to make the denial of service attacks	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	SEC vs. Scott Flynn www.sec.gov/litigation/admin/34-41102.txt	In a typical touting fraud, the defendant Flynn, a former stockbroker convicted of securities fraud in another matter, used spam to spread information about certain companies, without properly disclosing the receipt of compensation from those companies. The SEC alleged that unbeknownst to investors, Mr. Flynn spread information through his company, Strategic Network Development, Inc., without disclosing cumulative compensation of at least USD 183,200 in cash and 322,500 shares of stock from at least ten of the companies.	SEC Act of 1934	The SEC instituted cease and desist proceedings against the defendant. for violations of the anti-touting provisions of the federal securities laws. Outcome pending.	Unknown	Unknown
	SEC vs. Smith www.sec.gov/litigation/litreleases/lr18130.htm www.sec.gov/litigation/litreleases/lr18130.htm	Defendant admitted to conducting two fraudulent investment schemes through websites and spam email during 2002. The SEC charged him with fraudulently raising USD 102,554 by falsely guaranteeing double-digit monthly returns on two websites and in approximately nine million spam e-mail messages.	SEC Act of 1934, Rule 10-b(5)	Defendant consented to an order requiring him to pay USD 107,510 in disgorgement and pre-judgment interest and enjoining him from further violating the Securities laws	Unknown	Unknown
	SEC vs. 2DoTrade www.sec.gov/litigation/litreleases/lr18381.htm	The defendants engaged in a fraudulent scheme in which they artificially pumped 2DoTrade's stock with false press releases in spam e-mail linked to a fraudulent website and then illegally dumped millions of shares into the inflated market	Sections 5(a), 5(c), and 17(a) of the Securities Act of 1933 and sections 10(b) and 13(a) of the Securities Exchange Act of 1934.	Pending. The SEC seeks permanent injunctions, disgorgement of ill-gotten gains with pre-judgment interest, and civil money penalties against all the defendants	Unknown	Unknown
	SEC vs. Garst www.sec.gov/litigation/litreleases/lr18381.htm	Defendant allegedly sent a large number of unsolicited "spam" e-mail messages containing false and misleading statements concerning the product, revenue sources and business relationships of one of the touted issuers, as well as her stock-picking track record and the trading intentions of the persons responsible for the e-mail messages. Finally, the spam did not disclose cash compensation paid to her by the statutory underwriter.	Sections 10(b)5 of the Securities Exchange Act of 1934 and, and violated Section 17(b) of the Securities Act of 1933	Pending. The SEC seeks disgorgement of payments plus reasonable interest.	Unknown	Unknown
	SEC vs. Rice www.sec.gov/litigation/litreleases/lr17377.htm	Defendant allegedly carried out "pump and dump" schemes to manipulate the stock of four companies, including his own. The schemes for all four companies involved issuing unsolicited fraudulent e-mail messages. The false statements concerned, among other things, his company's product (purportedly an advanced Internet search engine), its revenue sources and business relationships with third parties, as well as his stock-picking track record and trading intentions.	Sections 10(b) of the Securities Exchange Act of 1934 and Section 17(b) of the Securities Act of 1933	Defendant consented to an order enjoining future violations of Securities laws and directing him to pay disgorgement and prejudgment interest	Unknown	Unknown

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Kalvin P. Schmidt www.ftc.gov/opa/1998/07/meganet.htm	Defendant sent spam e-mail to consumers directing them to websites, which promoted a chain letter based pyramid investment scheme. The scheme was based on false and unsubstantiated earnings claims.	§5(a) FTC Act	The FTC settlement bans Schmidt from participating in any chain letter schemes or pyramid sales schemes, and requires him to have a basis for any earnings claims. Schmidt would need evidence to substantiates any representation about the income, profits, or sales of any marketing plan or program or any material fact. Finally, the settlement contains various recordkeeping requirements.	Unknown	Unknown
	FTC vs. Dixie Cooley, d/b/a DWC www.ftc.gov/opa/1998/10/operasetl-3.htm	Defendant used email to scam consumers into believing that he could restore their creditworthiness for a fee. Sometimes charging more than USD 1,000, defendant purported to guarantee consumers they could remove negative information from their credit reports -- even if the negative information was accurate and timely. But, these companies cannot remove legitimate negative information and, where there are actual errors in credit reports, consumers have the legal right to have those corrected for free most of the time.	FTC Act and the Credit Repair Organizations Act (CROA)	Defendant ordered to pay USD 15,451.75 in consumer redress	Unknown	Unknown
	FTC vs. Epic Resorts, LLC www.ftc.gov/opa/2000/08/travelunravel.htm	Defendants allegedly marketed travel packages through spam that misled consumers by failing to disclose the actual cost, or concealing that they had to attend one -- and possibly more -- timeshare presentations.		The FTC sought redress for consumers.	Unknown	Unknown
	FTC vs. Associated Record Distributors, Inc www.ftc.gov/opa/2002/06/bizopswe.htm	Defendants sent spam email promoting false work at home opportunities. The promotions exaggerated earnings potential and assistance that respondents would receive.	Franchise Rule	FTC sought consumer redress, civil penalties, and a permanent halt to the deceptive claims.	Unknown	Florida Police Department assisted the FTC in the case.
	FTC vs. NetSource One	No further information available.				
	United States vs. A. James Black www.ftc.gov/opa/1999/02/consumerweek2.htm	Defendants advertised fraudulent services through email using claims such as "BRAND NEW CREDIT FILE IN 30 DAYS". The firms sold instructions to consumers how to substitute federally-issued, nine-digit employee identification numbers or taxpayer identification numbers for social security numbers, and use them illegally to build new credit profiles that would allow them to get credit they may be denied based on their real credit histories.	Credit Repair Organizations Act and the FTC Act	Unknown	Unknown	Department of Justice filed 3 cases and the FTC 14

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	United States vs. David Story www.ftc.gov/opa/1999/05/id21a4.htm	Approximately same facts as above.	Credit Repair Organizations Act and the FTC Act	Unknown	Unknown	DOJ and US Potal Inspection Service.
	United States vs. PVI, Inc. www.ftc.gov/opa/1998/09/vendup2.htm	The defendant made oral and written earnings claims to potential investors about digital photo vending machines via spam e-mail, but failed to provide either a basic disclosure document or an earning claims document.	Franchise Rule	Unknown	Unknown	DOJ filed the case at the request of FTC.
	FTC vs. LS Enterprises www.ftc.gov/opa/1999/04/spam2.htm		§5(a) FTC Act			
	FTC vs. Tim Cho Investment Corporation and Timothy Cho www.ftc.gov/opa/2001/03/cho.htm		§5(a) FTC Act			
	FTC vs. TrendMark International, Inc. www.ftc.gov/opa/1998/06/trendmrk.htm		§5(a) FTC Act			
	FTC vs. Ralph Lewis Mitchell, Jr. www.ftc.gov/opa/1999/02/consumerweek2.htm					
	FTC vs. Reverseauction.com, Inc www.ftc.gov/opa/2000/01/reverse4.htm					
	FTC vs. Rosalind Leahy www.ftc.gov/opa/2002/11/netforce.htm					

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. Sandra L. Rennert, et al. www.ftc.gov/opa/2000/07/iog.htm					
	FTC vs. Scott d/b/a Cyber Data	No further information available.				
	FTC vs. Seasilver USA, Inc. et al. www.ftc.gov/opa/2003/06/seasilver.htm					
	FTC vs. StuffingforCash.com Corp www.ftc.gov/opa/2002/07/mwnetforce.htm					
	FTC vs. West Coast Publications, LLC www.ftc.gov/opa/1999/9905/id21a4.htm					
	FTC vs. Yad Abraham ftc.gov/os/2003/08/idpsettlementabrahamstip.pdf					
	FTC vs. Nancy H. Merrill www.ftc.gov/opa/2002/11/netforce.htm					
	FTC vs. Nia Cano, et al. www.ftc.gov/opa/1997/11/cdi.htm					

	Case	Summary	Laws under which action was brought	Outcome / Status	Cross-border elements	Co-operation obtained
United States	FTC vs. One or More Unknown Parties www.ftc.gov/opa/2003/01/idpfinal.htm					
	FTC vs. Para-Link International, Inc., et al. www.ftc.gov/opa/2000/10/paralink.htm					
	FTC vs. Cliff Cross and d/b/a Build-It-Fast www.ftc.gov/opa/1999/02/consumerweek2.htm					
	FTC vs. D Squared Solutions www.ftc.gov/opa/2003/11/dsquared.htm					
	FTC vs. David Martinelli, Jr. www.ftc.gov/opa/1999/07/dpmarket.htm					