FEDERAL TRADE COMMISSION
OFFICE OF INTERNATIONAL AFFAIRS

600 Pennsylvania Avenue N.W.
H-494
Washington, D.C. 20580

Tel: (202) 326-2777
E-mail: swatson@ftc.gov

February 15, 2011

Via e-mail

Stephen Weber
Senior Investigator
Anti-Spam Team
Australian Communications and Media Authority
P.O. Box 13112 Law Courts
Melbourne Vic 8010
Australia

Dear Stephen:

Thank you for the opportunity to review the Australian Communications and Media Authority's (the ACMA) best practice case study on spam. The case study illustrates the significant progress the ACMA has achieved in protecting Australian consumers from unsolicited spam messages, including those sent to mobile devices. We understand that you are soliciting informal comments on the case study related to the challenges facing spam regulators, spam reporting and consumer education initiatives, and the ACMA's role in international spam cooperation.[1] Accordingly, our comments below focus on these issues.

As you know, the Federal Trade Commission (FTC) is an independent agency of the U.S. government that promotes competition and protects consumers. As part of its consumer protection mission, the FTC enforces a wide range of statutes that, among other things, prohibit unfair or deceptive acts or practices.[2] In particular, the FTC increasingly has used its enforcement authority to address consumer protection issues arising in the online world, including Internet fraud, spyware, and spam. In 1997, the FTC began bringing spam-related enforcement actions under its general authority to combat deceptive and unfair practices under the FTC Act.[3] In 2003, the agency received additional legislative authority—the CAN-SPAM

[1] The comments provided in this letter are solely staff comments and do not reflect the views of the Commission or any individual Commissioner.
[2] *See* 15 U.S.C. § 45(a).
[3] *See id.*

Act of 2003—to address harm caused by spam.[4] Since 1997, the FTC has brought over 90 law enforcement actions involving spam under these Acts. In addition to enforcement actions, the FTC has adopted a multi-faceted approach to address spam, including educating consumers and businesses, conducting research on spam harvesting and anti-spam filters, hosting workshops for relevant stakeholders, and spurring the development of industry-driven technology.[5]

In light of this experience, we are familiar with the challenges facing authorities that enforce anti-spam laws. As the tools to disseminate spam messages have evolved, we understand that one of the most significant challenges to spam enforcement is the use of botnets—networks of hijacked computers that enable spammers to send large volumes of spam anonymously and remotely.[6] In 2009, the FTC shut down a malicious botnet by bringing an enforcement action against a rogue ISP in *FTC v. Pricewert*.[7] The ISP, which operated under the name 3FN, deployed and operated botnets, recruited bot herders, and hosted the botnet command-and-control servers—the computers that relay commands from the bot herders to the compromised computers. The botnets hosted by 3FN were used to distribute spam, spyware, and other malicious content. According to industry reports, the FTC's enforcement action against 3FN resulted in an immediate and significant, albeit temporary, drop in spam levels. In pursuing this case, the FTC cooperated with other government agencies, the private sector, and academia, which all provided useful evidence.

Given this experience, we would be interested in learning more from the ACMA about the strategies it has adopted to deal with botnes, and whether there has been useful cooperation with Internet Service Providers (ISPs) in Australia to tackle this problem. It would be useful to include more information about the ACMA's strategic approach to addressing botnets in the case study.

In addition to the deployment of botnets, another challenge that we have encountered is that spam is increasingly a vector for criminal activity.[8] As a result, criminal authorities, such as the Federal Bureau of Investigation and the U.S. Department of Justice, have pursued a number of enforcement actions and initiatives to address spam used to further criminal activity. Although the FTC does not have jurisdiction over criminal matters, it has created a Criminal Liaison Unit, known as CLU, to work with criminal authorities in instances in which the conduct at issue in an FTC investigation or enforcement action may also violate criminal statutes. The ACMA's case study does not mention the challenges associated with spam disseminated to further criminal purposes, or its cooperation with Australian criminal authorities on spam issues. It might be useful to understand whether there are any intergovernmental cooperative arrangements in Australia that exist in this area.

The e-mail architecture itself also presents a fundamental challenge, as its open structure makes it susceptible to manipulation and allows fraudsters to use techniques such as "spoofing" or open relays to remain anonymous. To combat this problem, the FTC has encouraged industry

---

[4] *See* The CAN-SPAM Act of 2003, 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037.
[5] *See* FTC, Spam Summit: The Next Generation of Threats and Solutions, at 5 (November 2007), *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf [hereinafter Spam Summit Report].
[6] *See id.*
[7] *See FTC v. Pricewert LLC*, No. 09-CV-2407 (N.D. Cal. filed June 1, 2009), press release *available at* http://www.ftc.gov/opa/2009/06/3fn.shtm.
[8] *See* Spam Summit Report, *supra* note 5, at 3.

to develop domain-level authentication technologies that would provide a method for identifying the true origin of an e-mail.[9] In 2004, the FTC, in conjunction with the National Institute of Standards and Technology, co-hosted the Email Authentication Summit, which brought together government representatives, technologists, ISPs, computer scientists, and businesses that operate their own mail servers to discuss the development, testing, and deployment of authentication standards to reduce spam.[10] Although the ACMA case study mentions that it has encouraged spam filtering, it does not refer to the issue of authentication. It would be useful to know whether the ACMA has considered e-mail authentication and, if so, whether it has made any recommendations with respect to the adoption of authentication technologies.

As the case study indicates, one helpful tool in investigating spam enforcement actions has been the creation of spam reporting centers. The case study describes the ACMA's spam reporting initiatives, which allows consumers to report spam, including SMS spam, to the ACMA. The case study also highlights the ACMA's efforts in encouraging ISPs to use spam-filtering software. It might be useful if the ACMA could share data about the volume of spam it receives via its reporting mechanisms, and how the data are used with respect to enforcement actions. In addition, it would be useful to know whether the ISPs provide a spam reporting mechanism to use for filtering. Further, it would be helpful to learn whether ISPs forward consumer complaints to the ACMA.

Similarly, the FTC has provided a spam reporting mechanism to consumers for over ten years, and consumers can forward spam messages, including those received on mobile devices, to the FTC's spam reporting e-mail address--spam@uce.gov. In fiscal year 2010, consumers sent 44 million messages to the FTC's spam database. In May 2010, the FTC made the spam database data available on its Consumer Sentinel Network, an online tool administered by the FTC that provides consumer complaint data to state, federal, and foreign law enforcement agencies.[11] The FTC also conducts outreach to ISPs, which may forward consumer complaints to the agency.

In connection with the spam reporting initiatives, the case study emphasizes the ACMA's consumer education efforts. The case study describes the ACMA's collaborative approach to consumer education, noting that it works with industry bodies, consumer groups, and other government agencies to develop integrated and effective messages to consumers. Similarly, the FTC has acknowledged that consumer and business education is a key component of its anti-spam program. In particular, the FTC's consumer education initiatives have involved considerable outreach to other U.S. and foreign agencies, consumer groups, and the private sector with the aim of developing coordinated consumer education campaigns that can be disseminated more widely. For example, in April 2008, the FTC hosted a roundtable discussion that was solely devoted to improving consumer education about phishing e-mail scams. Approximately 60 experts from business, government, the technology sector, consumer advocacy community, and academia participated in the roundtable, which generated ideas to use website landing pages as educational tools and enlisted participants from the various

---

[9] *See* FTC, National Do Not Email Registry, A Report to Congress (June 2004), at 35-36, *available at* http://www.ftc.gov/reports/dneregistry/report.pdf.

[10] *See* http://www.ftc.gov/bcp/workshops/e-authentication/index.shtm.

[11] *See generally* http://www.ftc.gov/sentinel.

communities to distribute consumer education videos through new channels, such as mobile devices and video games.[12]

The FTC also collaborated with several relevant stakeholders, including consumer groups, industry associations, and over 10 other government agencies, when it launched OnGuardOnline.gov, an interactive online tool that provides consumers with practical tips to help them prevent Internet fraud, secure their computers, and protect their personal information.[13] The website, which features topics ranging from securing Wi-Fi networks to identity theft, includes materials that describe potential e-mail scams and advises consumers on threats posed by botnets. OnGuardOnline.gov is designed to allow others to download its interactive modules and place them on their own websites, which facilitates the sharing of the educational information with more consumers—both domestically and internationally. Since the launch of OnGuardOnline.gov and AlertaenLínea.gov, its Spanish-language counterpart, in September 2005, almost 11 million visitors have accessed these sites for information about computer security.[14] Notably, in October 2009, President Obama directed people to OnGuardOnline.gov in a presidential proclamation and video on the White House blog about National Cyber Security Awareness Month.[15] If the ACMA does not already employ a similar tool, the FTC could cooperate with the ACMA to promote the use of OnguardOnline.gov in Australia.[16]

As the case study highlights, the ACMA's multi-faceted approach to spam enforcement also includes a key focus on international cooperation. Indeed, the ACMA has emerged as a global leader on international spam enforcement cooperation. In 2004, the FTC and the ACMA, along with other foreign agencies, signed a Memorandum of Understanding on mutual cooperation in the area of spam enforcement. Pursuant to that agreement, the FTC has worked closely with the ACMA in several international spam matters. The ACMA's investigative assistance has helped to facilitate successful law enforcement actions against illegal spammers, including the *Atkinson* case referenced in the case study.

In addition, as the case study indicates, the ACMA has been a member of the London Action Plan, a global public-private anti-spam network, since its inception in 2004. The FTC, which co-hosted the launch of the London Action Plan with the UK Office of Fair Trading in 2004 and served as a member of the Secretariat since its creation, is also a very active member of the enforcement network. In this capacity, the FTC has had the opportunity to work with the ACMA on several of the London Action Plan's projects. The ACMA has helped coordinate global conferences, delivered presentations to a diverse group of conference participants, and trained law enforcement officials from agencies all over the world. Notably, the annual London Action Plan conference that the ACMA hosted in Melbourne last year provided a unique opportunity for the agency to showcase the breadth of its expertise in anti-spam issues to an

---

[12] *See* FTC, Roundtable Discussion on Phishing Education, A Staff Report by the Federal Trade Commission's Division of Consumer and Business Education and Division of Marketing Practices (July 2008), *available at* http://www.ftc.gov/os/2008/07/080714phishingroundtable.pdf.

[13] *See* http://www.onguardonline.gov/.

[14] *See* FTC, Net Cetera OnGuardOnline.gov's Internet Safety Campaign for Children, A Report to Congress, at 2 (March 2010), *available at* http://www.ftc.gov/os/2010/03/100331netcetera-rpt.pdf.

[15] *See id.* at 4.

[16] The OnGuardOnline.gov materials are intentionally designed for other entities to copy them wholesale or adapt them as necessary for their respective communities.

international audience. In short, the ACMA's participation in the London Action Plan has been invaluable in furthering the goal of international spam enforcement cooperation.

As a founding member of the Seoul-Melbourne MOU Group, an anti-spam network in the Asia-Pacific region, the ACMA continues to be active in establishing and fostering relationships with foreign agencies to help reduce the sending of unsolicited spam messages. The ACMA has been instrumental in serving as a liaison between the Seoul-Melbourne MOU Group and the London Action Plan, providing valuable insight on how members of the respective networks can work together.

In summary, there are several similarities between the ACMA's and the FTC's strategic approaches to enforcing anti-spam laws, as both agencies incorporate enforcement actions, spam reporting, consumer education, and international cooperation into their respective programs. As a result, it provides a useful opportunity to share best practices. We hope that the comments provided above are helpful to you as you evaluate your anti-spam program, and we remain available to answer any questions.

Sincerely,

Shaundra Watson
Counsel for International Consumer Protection
U.S. Federal Trade Commission