

Asia/Pacific

JUSTIN G. PERSAUD AND STEVE SAUNDERS*

This article highlights selected legal developments in the Asia/Pacific region during 2011.¹

I. Asia Region Funds Passport

In Asia, there is currently no single agreement that would allow an investor to invest in several markets through one vehicle. At the 2011 Honolulu Asia Pacific Economic Cooperation (APEC) meeting, finance ministers endorsed the pilot Asia Region Funds Passport (ARFP) structure,² a suggestion first proposed by Australia at the October 2010 APEC meeting in Kuala Lumpur. Australia had set a two-stage process to implement the proposal.³ First, the Australian Securities and Investments Commission (ASIC)⁴ would negotiate bilateral mutual recognition agreements with key jurisdictions in the region. Second, once the bilateral agreements were in place, governments and agencies in the region would work to develop these into a multilateral Passport system.⁵

The ARFP draws its inspiration from the Undertakings for Collective Investment in Transferable Securities (UCITS) in the European Union (EU). The idea behind ARFP is

* Justin G. Persaud, a LL.M. candidate in securities law at Osgoode Hall Law School, York University, Toronto, Canada, authored the section on the Asia Region Funds Passport and served as committee editor. Steve Saunders, a lecturer at the University of Toyama, Japan, prepared the section on Japan.

1. For developments during 2009, see Manish Dhingra et al., *Asia/Pacific*, 44 INT'L LAW. 595 (2010). For developments in the Asia/Pacific region during 2010, see William A. Herbert et al., *Asia/Pacific*, 45 INT'L LAW. 455 (2011). The Asia/Pacific Committee of the ABA Section of International Law covers all countries in the Asia/Pacific region, including Afghanistan, Australia, Bangladesh, Bhutan, Brunei, Cambodia, the Cook Islands, Fiji, Indonesia, Japan, North Korea, South Korea, Laos, Malaysia, the Federated States of Micronesia, Myanmar (Burma), Nepal, New Zealand, Pakistan, the Republic of Palau, the Philippines, Singapore, Sri Lanka, Thailand, and Vietnam. The section also has committees on China and India. For developments in India during 2012, see Hanishi T. Ali et al., *India*, 46 INT'L LAW. 553 (2012). For developments in China during 2012, see Ying Deng et al., *China*, 46 INT'L LAW. 517 (2012).

2. *APEC Finance Ministers Consider UCITS-Style Asia Region Funds Passport*, GCAUSTRALIAN (Nov. 16, 2011), <http://australia.globalcustodian.com/news/Fund-Administration/APEC-Finance-Ministers-Consider-UCITS-Asia-Region-Funds-Passport/41233>.

3. AUSTRALIAN FINANCIAL CENTRE FORUM, AUSTRALIA AS A FINANCIAL CENTRE: BUILDING ON OUR STRENGTHS (Nov. 2009), available at <http://www.mercari.com.au/media/AFCF.pdf>.

4. *Id.*

5. *Id.*

to provide for a system of marketing registered funds across participating Asian borders. The ARFP will establish a set of regulations that will be consistent among various Asian countries. The agreement would require common structural requirements and investment regulations. ARFP's structural requirements would allow funds to be passported across jurisdictions. Structural requirements include registration arrangements, licensing arrangements, and custodian arrangements. Registration arrangements would allow a fund designated as a "passport compliant fund" in its home jurisdiction to be exempt from registration requirements in other participating passport countries.⁶ Agreements among licensing arrangements would allow a fund manager holding a license in its home jurisdiction to offer passport compliant funds to investors in other passport countries without obtaining a license there. The system would include requirements regarding separate custodianship of a fund's assets.

There are several issues regarding the direction of investment regulations. Investment rules are being drafted to take into account to what degree they should replicate UCITS rules. While an Asian passport system that replicates the regulatory structure of UCITS would allow for easier transactions between Europe and Asia, UCITS is much more restrictive in its regulation of funds products. Other investment regulations that would need to be worked out include the following issues: eligible investment asset classes; offer document conditions; limits on leverage; liquidity requirements; and investor protection and dispute resolution procedures.

Although there are numerous benefits to this multilateral agreement, it is not without a substantial number of challenges, including inconsistent tax treatments, market maturity, and currency issues. Despite these hurdles, market orientation is applying pressure for regulatory harmonization.

The passport system will ultimately begin with a multilateral agreement among the leading Asian markets. It has been proposed that a small group of leader countries should mutually agree to set regulations for an ARFP and encourage other countries to participate.⁷ Given that APEC recently endorsed this pilot regime at the 2011 Honolulu meeting, it will become much clearer as to how this regime will develop moving forward in 2012.

II. Japan's New Cyberlaw

The Japanese Diet (the National Parliament) passed a law in 2011 that makes it a crime to send spam mails or computer viruses in Japan.⁸ The law may have been passed in part after several servers in Japan were used as part of a "botnet" attack in March 2011, an attack believed to have originated in North Korea.⁹ The new law makes spamming a

6. *Id.*

7. *APEC Finance Ministers Consider UCITS-Style Asia Region Funds Passport*, *supra* note 2.

8. *Don't Spam in Japan: Law against 'Viruses' and Spam Emails Carries Up to Three Years in Jail Time*, DAILY MAIL REPORTER (June 21, 2011), <http://www.dailymail.co.uk/news/article-2005891/Japan-passes-law-viruses-spam-emails-carrying-years-jail-time.html>.

9. Yomiuri Shimbun, *Japan PCs 'Joined' Cyber-Attacks* (Sept. 23, 2011), <http://www.yomiuri.co.jp/dy/national/T110922006331.htm>.

more serious crime than previously.¹⁰ “Acquiring” or storing a virus can result in a ¥300,000 fine (approximately US\$3,895) and two years in prison.¹¹ “Distributing” the virus can result in a three-year prison sentence and a ¥500,000 fine (approximately US\$6,493).¹² Sending emails containing pornographic images to random email users is now also a crime.¹³ With the passage of the new law, Japan would now be able to join the Budapest Convention on Cybercrime.¹⁴ Japan has signed the Convention but has not yet ratified it.¹⁵

Other governments may look to the Japanese law to see how well it works, but the law appears to have been written by persons who did not understand how computer viruses are spread. Among other things, it is entirely possible for a person to have computer malware installed on their computer without being aware of it. A computer could be used as part of a botnet attack and that person could be held liable under the new law even though they did not know the virus was on their computer. The point of a really good computer virus is that it can hide itself deep in the operating computer and is difficult to detect. During the debate on the law, some expressed concern that one effect of the law would be to breach the privacy of computer users since the government can now seize the logs of ISP providers in Japan. Another problem with cracking down on spam mails in Japan is that almost all of them are sent from countries outside of Japan in the first place. Also not addressed is the issue of persons who use Japanese email servers to send out spam mails or scam email formats.

In an ironic twist, an attack on the Japanese Parliament’s website launched from a Chinese server in October 2011 resulted in data loss as hackers gained access to the emails of parliamentarians including strategically sensitive information, such as defense policy.¹⁶ The attack was made possible because a member of the Lower House opened an email attachment with a virus in July on a personal computer.¹⁷ The member later connected to the Parliament’s system and spread the virus, which was able to breach the network’s antivirus firewall, and allowed the data and emails to be accessed.¹⁸ Under the new law, the member would likely be guilty of a crime although there were no indications that the member would be charged.¹⁹

A further gap between theory and reality was revealed when viruses were also found on the computer systems at several Japanese overseas diplomatic missions.²⁰ A backdoor computer virus was installed on the computer system that may have compromised sensi-

10. *Don't Spam in Japan: Law against 'Viruses' and Spam Emails Carries Up to Three Years in Jail Time*, *supra* note 8.

11. *Id.*

12. *Id.*

13. *Id.*

14. EUR. CONSULT. ASS., *Convention on Cybercrime*, Doc. No. 185 (2004), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

15. *Id.*

16. *Cyber-Attack from Server in China Targets Lower House*, THE ASAHI SHIMBUN (Oct. 25, 2011), http://ajw.asahi.com/article/behind_news/AJ2011102515710.

17. *Id.*

18. *Id.*

19. *Id.*

20. Yomiuri Shimbun, *Diplomatic Computers Hit: 'Backdoor' Virus Found at Japanese Missions in 9 Countries*, THE DAILY YOMIURI (Oct. 27, 2011), <http://www.yomiuri.co.jp/dy/national/T111026005025.htm>.

tive information.²¹ Computer systems at a major Japanese defense contractor were also found to have been infected with viruses in October 2011. Investigations are continuing.

21. *Id.*