
Australian Payments
Clearing Association

# Submission to the Inquiry into Cyber Crime

**July 2009**

**Industry Policy,**
**Australian Payments Clearing Association Limited** ABN 12 055 136 519
Level 6, 14 Martin Place, Sydney NSW 2000 Telephone +61 2 9221 8944
Facsimile +61 2 9221 8057 **www.apca.com.au**

**Contents**

# 1. EXECUTIVE SUMMARY

1. The Australian Payments Clearing Association Limited (APCA) welcomes the opportunity to provide a submission to the Inquiry into Cyber Crime.

2. In this submission, APCA will provide background information on a specific typology of cyber crime, namely online card fraud. APCA endorses any work of the Committee that will identify the full scope of other cybercrime typologies and identify where there are gaps in cybercrime prevention.

3. APCA publishes data on fraud across the Australian payments system which indicates the emergence of Card Not Present fraud, of which a large proportion is online card fraud, as a significant issue facing card payments.

4. At the same time, it is important to recognise that Australian fraud prevention efforts perform relatively well by global standards. It is also an area that is actively managed and monitored by Australian issuers and global card schemes, and where there are strong incentives for continued prevention effort.

5. APCA believes that reliable statistical information is an important contributor to systematic fraud minimisation. This may be particularly difficult in the virtual world, given its inherent complexity, diversity and changeability. The committee may wish to consider how best to address this gap.

# 2. BACKGROUND

## *2.1. Inquiry into Cyber Crime*

6. On Wednesday, 13 May 2009, the Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy, asked the House Standing Committee on Communications to inquire into and report on the nature and incidence of cyber crime in Australia.

7. The Committee issued an invitation for interested persons and organisations to make submissions addressing the terms of reference by Friday, 26 June 2009. APCA received an invitation on 30 June 2009 with a response date of 17 July 2009 which has been extended to 24 July 2009.

8. Cyber Crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a criminal activity[1]. These categories are not exclusive and many activities can be characterised as falling in one or more areas.

9. APCA understands that the focus of the Committee's inquiry is broad, covering a variety of criminal activity that can be perpetrated on-line. APAC believes that an essential element of this inquiry should be to firstly identify the typologies of cybercrime and then prioritise these typologies in terms of their fiscal and social costs. Once this has been established, the required work to address this crime is easier to develop.

10. Our purpose in this submission is to provide a background on the work the payments industry is undertaking to combat one particular type of cybercrime typology, payment card fraud, a small but highly visible part of overall cyber crime, and one of the few areas where reasonably comprehensive and reliable Australian statistics are available.

## *2.2. About APCA*

11. The Australian Payments Clearing Association Limited (APCA) was established in 1992 as a mutual self-regulatory organisation for banks, building societies, credit unions and other payments organisations. APCA is the primary vehicle in Australia for payments industry collaboration, with a mandate to improve the safety, reliability, equity, convenience and efficiency of the Australian payments system.

12. APCA has specific accountability for key parts of the Australian payments system, particularly payments clearing operations. It is currently responsible for the efficient administration and self-regulation of the following five clearing systems:

[1] See for example definition in the Macquarie Concise Dictionary (3rd Edition) and Wikipedia http://en.wikipedia.org/wiki/Cyber_crime

(a). Australian Paper Clearing System (cheque and other paper based payments);

(b). Bulk Electronic Clearing System (direct entry payments, including some telephone and internet banking transactions);

(c). Consumer Electronic Clearing System (ATM and EFTPOS debit card transactions);

(d). High Value Clearing System (SWIFT/PDS payments); and

(e). Australian Cash Distribution and Exchange System (wholesale cash transactions).

13. More information about APCA can be found at: www.apca.com.au.

## *2.3. APCA's role in fraud prevention*

14. APCA's strategic focus is on improving the underlying payments system, including its security and safety. APCA's fraud committee monitors payments fraud trends and APCA participates in industry-wide initiatives to counter fraud.

15. Payments fraud prevention activities can be seen to operate at four different levels:

- The first level focuses on actions to be taken by the end user - either the customer or the merchant. Cardholders can ensure they protect cards and PIN information; merchants can ensure staff follow work practices that will discourage fraud attempts.

- The second level is at the financial institution: implementing measures to protect the institution's customers. At this level, Australian institutions have invested significantly in fraud detection and risk management systems.

The remaining two levels focus more widely:

- The third operates at the scheme level (for example specific measures developed and implemented separately by Visa and MasterCard to reduce online fraud).

- The fourth operates at an industry wide-level, encompassing financial institutions, government and law enforcement agencies, merchants, technology providers and customers. It is in this area that APCA is working to improve fraud prevention efforts and promoting cross industry initiatives to reduce the fraudulent use of online payments systems.

16. APCA began publishing fraud statistics in November 2006 as part of the industry's commitment to improve disclosure and to help protect consumers and businesses in

Australia. Statistics are published every six months, measuring the total amount and value of cheque, debit card, credit card and charge card fraud losses.

17. APCA has worked to implement standards, guidelines and introduce coordinated activities to reduce payments fraud, particularly for cheques, ATM and EFTPOS.

18. Ongoing industry coordination by APCA, involving major issuers and schemes, is seeking to address CNP fraud.

# 3. ONLINE FRAUD

## *3.1. Trend Analysis*

19. On-line purchasing has increased markedly over recent years. According to a recent survey[2], the proportion of Australian internet users who made an online purchase increased from 62% in the second quarter of 2007 to 70% at the last quarter of 2008. When selecting a single, most preferred method for online payment, half prefer credit card while one quarter prefer PayPal and one in ten prefer Bpay.

20. In addition to the increase in the incidence of active online purchase for this quarter, the active Internet user population (from home or work) has also increased between October 2007 and October 2008 – from 9.8 million up to 10.4 million. This translates to an active shopping population of 7,301,000 during Q4 2008, up from 6,485,160 in Q4 2007.

21. Online card payments use a facility known as Card Not Present (CNP), in which the card number (and other data easily obtainable from the card itself) is used to verify the purchase.

22. The level of CNP fraud has been increasing over the last few years, both in Australia and worldwide. Some of this fraud is carried out over the telephone or through mail order, but the majority is online fraud. This is partly as a result of the increase in online card payments, but also due to greater activity by fraudsters. There have also been reports of highly-sophisticated criminal fraud rings operating in this space.[3]

23. It is difficult to counter this type of fraud since neither the card nor the cardholder is present when the transaction happens. Therefore methods normally available to authenticate the payment cannot be used in this case. These include checking the validity of the card using its physical security features, and checking that the customer is the genuine cardholder through a signature or PIN. The anonymity and speed of the Internet also makes it easier for criminals to perpetrate widespread fraud.

[2] Online Retail Monitor Quarterly, Quarter 4 2008, Nielsen Online.
[3] See, for example, "Fraud Ring Funnels Data From Cards to Pakistan", Wall Street Journal 11 October 2008 [http://online.wsj.com/article/SB122366999999723871.html]

24. APCA's most recent publication of payments fraud statistics in December 2008 has demonstrated the significance of CNP fraud in Australian card payments, and that such fraud is growing.

25. In the year to June 2008 CNP fraud cost the industry $63.5m compared to $40m the previous year and $27m the year before that. It currently accounts for 48% of the fraud value on Australian-issued credit and charge cards and 39% of fraud on all Australian-issued payments instruments. This compares with 31% and 19% respectively only two years previously. Such figures do, however, need to be considered in the context of increased online card payments.

26. This compares favourably with the UK (the only other jurisdiction that publishes its payments fraud statistics) where in 2007 CNP fraud cost £290.5m and constituted 54% of all the payment card fraud value.

27. Consumers are protected by the card schemes' zero liability policy and are not held liable if fraudulent transactions are made with their cards or account information. Instead, CNP fraud costs typically fall either on the merchant or the issuer, depending on what anti-fraud measures have been adopted by each party. In this way, the card schemes seek to incentivise industry participants to invest in fraud prevention.

### *3.2. Initiatives to Combat CNP fraud*

28. While the level of fraud to some extent reflects the vast increase in total CNP transactions, the Australian payments industry is working hard to counter this type of fraud on a number of levels.

29. On an individual basis (at the second level of fraud prevention referred to above), financial institutions undertake campaigns to educate customers on minimising fraud risks, such as protecting their PIN.

30. Individual institutions employ various techniques to identify and prevent fraudulent CNP transactions from being accepted. These include sophisticated pattern-analysis tools to identify transactions that stand out from a customer's normal payments pattern, thus allowing them to stop or check suspected frauds. Some card issuers also carry out separate checks, such as sending an SMS to the cardholder's mobile phone and asking for confirmation of the transaction.

31. The international card schemes have developed various measures to reduce CNP fraud. These include additional methods for authenticating cardholders during CNP transactions such as CVV2 (the additional verification number found on the card), plus the on-line authentication mechanisms: Verified-by-Visa and MasterCard's SecureCode. Take-up of these mechanisms is encouraged through the use of liability shifts, thus allowing merchants, in particular, to reduce their exposure to CNP fraud.

32. Recently Visa announced its 5 year plan to strengthen the security of the payments system in Australia. This plan includes three initiatives aimed at limiting CNP fraud including encouraging further take-up of Verified-by-Visa and CVV2, and encouraging higher levels of protection of card data at merchants.

33. At the industry level, the Payments Card Industry Data Security Standards (PCI-DSS) are aimed at minimising the amount of card and cardholder data held by merchants and acquirers and ensuring adequate security measures are used to protect any such data that is held. The industry is spending a significant amount of effort in helping merchants meet these standards.

34. In addition, various industry groups including APCA, the ABA, and the Australasian Cards Risk Council are promoting co-operation between the different players in reducing the levels of CNP fraud. This includes greater support of state and federal police, information sharing and consideration of co-ordinated industry plans to implement greater transactional security.

35. The importance to the industry of limiting CNP fraud is evidenced by the fact it was one of the items allocated a high priority during the joint APCA/ABA Fraud Industry Direction Workshop held in February 2008.

### *3.3. Other cybercrime typologies*

36. Internet banking fraud, including phishing, is also an important factor in cybercrime. APCA, however, is not addressing this broader topic within our submission because this has historically fallen outside our remit of payments. Nevertheless, it should be noted that APCA monitors the incidence of such crime though its Fraud Committee (while not collecting any detailed statistics on these types of fraud) and. the industry continues to develop initiatives to combat this type of fraud.

37. It is also worthwhile referring the Committee to extensive work being undertaken elsewhere in the industry. The Australian Bankers Association (ABA) and the Australian Federal Police have established the Joint Banking and Financial Sector Investigation Team to specifically investigate and close down phishing sites targeting Australian financial institutions; mule recruitment sites used to facilitate money laundering; and malware download sites.

38. The ABA has also developed a website in conjunction with the Federal Police promoting the protection of financial identity (www.protectfinancialidentitiy.com.au).

39. Because of the seriousness of cyber crime and the impact of this on the banking system, the remit of the APCA Fraud Committee has recently been extended to cover all payments fraud and other related fraud (such as internet banking) where industry co-operation is deemed worthwhile.

# 4. CONCLUSIONS

40. APCA is working with the industry to promote greater cohesion in the fight against, for example, online fraud, particularly in relation to CNP fraud. Other areas of cybercrime typology might not be so well measured and documented.

41. At a recent meeting of a body established by APCA called the Card Payments Forum[4], it was agreed that fraud prevention represented an area where enhanced cross industry collaboration was essential. APCA is currently investigating options for a fraud prevention strategy for consideration at the next Card Payments Forum meeting in September 2009.

42. Online card fraud is a growing global problem, but one where Australian fraud prevention efforts still performs relatively well by global standards. It is also an area that is actively managed and monitored by Australian issuers and global card schemes, and where there are strong incentives for continued prevention effort.

43. APCA keeps statistics on this area of fraud and is examining the feasibility of extending its collection into related areas, such as internet banking fraud. APCA believes that effective systematic prevention is greatly assisted by reliable statistical information about levels of fraudulent activity. Such information allows the calculation and allocation of value-at-risk, so as to drive cost-efficient prevention measures; it also provides important context for consumer education and awareness promotion, which can minimise opportunities for fraud at its source. In simple terms, what gets measured, gets managed.

44. This may be particularly difficult in the virtual world, given its inherent complexity, diversity and changeability. The Committee may wish to consider how to promote better understanding of cyber crime through identification of other cybercrime typologies, and, having established this, investigate prevention measures through the systematic collection of quantitative and qualitative data. We are happy to help the committee further if required.

*m:\dept\research policy\cyber crime enquiry\draft submission\final draft inquiry into cyber crime submission v.4.doc*

[4] The Card Payments Forum consists of senior representatives from key stakeholders in the card payments system. For more information on its scope and objectives, see www.cardpaymentsforum.com.au.