

## The four layers of fraud prevention


Fraudsters will always seek out the path of least resistance. They target vulnerabilities in individuals, property or financial institutions. The possibilities for fraudulent endeavour in payments systems are many and varied; fraudulent activities can be undertaken with little personal risk involved, at physical remove from the target, and with significant sums of money available as a reward.

Historically, Australian financial institutions have been very good at preventing payments fraud, especially when compared to other jurisdictions. As an example, at 24 cents in every \$1000, Australia's plastic card (debit, credit and charge card) rate of fraud is less than a third of that in the United Kingdom which remains the equivalent of about 90 cents for every \$1000.

This does not mean Australia can be complacent. As other jurisdictions improve their defences there will be an inevitable shift by criminals as they go forum shopping for weaker defence payment systems. Fraudsters are never restricted geographically in this age of the internet.

According to the Australian Institute of Criminology, fraud comprises 16% of the total annual cost of crime in Australia. This is a cost that cannot be ignored, irrespective of the fact that percentage-wise, it may be higher elsewhere.

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.



*Fraud (prevention) is big business. Is the payments industry doing enough?*

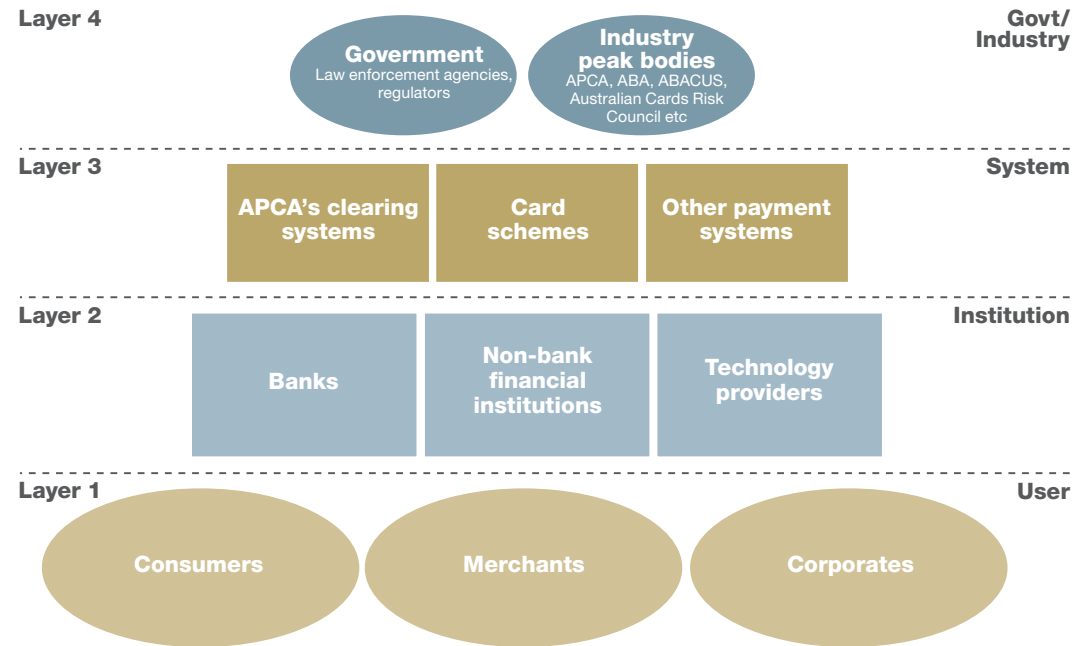
## Views // The four layers of fraud prevention (continued)

To date, payments fraud prevention initiatives in Australia have largely taken place at the first three levels. There have been fourth level type industry forums such as the Australian Bankers' Association's (ABA) Financial Crimes Steering Group and APCA's Fraud Committee, but these have not attracted much attention in recent times. This article seeks to examine the desirability of enhanced industry effort as a complementary measure alongside existing (and so far successful) effort on the other three levels.

Examples of fourth level type fraud prevention activities include:

- an education campaign run as a joint initiative between the ABA and the Australian High Tech Crimes Centre;
- the Joint Banking Financial Services Team, which is a centralised body set up to provide a point of contact for law enforcement agencies to obtain information on online banking fraud; and
- publication by APCA of industry-wide data on cheque and card fraud, in line with current practice in the United Kingdom.

In addition, some of Australia's major financial institutions are working together to create the Trust Centre: a central service set up to facilitate user identification and hence cut the level of identity fraud currently associated with false applications for bank accounts.



However, the question is whether more should be done to enhance fraud prevention and detection in Australia through a more coordinated, industry-wide approach? If the answer is yes, then how should this be done? An important element of this would be to improve interaction between the different players in the industry, including financial institutions, government and law enforcement agencies, merchants, technology providers and customers, as occurs in many overseas jurisdictions.

There are two main obstacles to fourth level effort. First, the business case for investment in fraud prevention initiatives is much easier to establish when that initiative is specific to a single institution where the costs and projected savings are clear. By contrast, translating overall industry costs and benefits of collective industry efforts into predicted net benefit for a critical mass of individual institutions, each of which has different fraud profiles and systems, can be very difficult.

Second, there is the problem of comparative advantage. Any successful industry effort reduces total fraud costs, but will not by definition, confer any significant competitive advantage on any one institution or class of institutions. Given an investment choice between an industry effort and one that will confer competitive advantage on a single institution, it will be difficult to persuade business managers to opt for the former.

Despite this, overseas experience suggests that as a complement to other efforts, industry cooperative effort is valuable in long-term fraud prevention.

An example of effective cross industry coordination in preventing payments fraud can be found in France, where the Observatory for Payment Card Security (OPCS) was established in 2001 to promote dialogue and exchange of information between all parties that have an interest in the security and smooth functioning of the French card payment systems. The typical work undertaken by the OPCS relates to the identification and analysis of card fraud activity, facilitating ongoing evaluation of the potential impact of such fraudulent activity on card and device security standards and timely dissemination of information on the latest modus operandi being utilised by criminals.

In the United Kingdom, there has been a wholesale shift in attitude to payments fraud prevention, spurred by the substantial level of payments fraud encountered. The best example of this is the cooperative approach taken by industry bodies and law enforcement agencies to establish the Payments Industry & Police Joint Intelligence Unit, an industry-funded agency staffed by both industry experts and law enforcement officers. This effectively combines expertise in payment systems and financial crimes with the objective of preventing and detecting payments fraud within the one office. In such circumstances, by having an industry wide independent body closely cooperating with law enforcement agencies, sensitivities relating to competition and commercial confidence between financial institutions are unlikely to arise, and protection of the entire industry is undertaken in a coordinated manner by a central body.

In both France and the United Kingdom, a combination of information sharing and technological innovation are being used to combat payments fraud.

**Views // The four layers of fraud prevention** (continued)

Of course, there are significant differences between the Australian payments system and those of France and the United Kingdom, therefore these types of measures may not be appropriate within the Australian environment, or would at the very least need to be suitably tailored. Irrespective of environmental differences, however, lessons can be learned from the cooperative nature of these initiatives where financial institutions and law enforcement officers combine their expertise to successfully combat fraud, complementing fraud prevention strategies pursued by customer education, financial institutions' internal preventative measures and scheme measures.

From such cooperation, industry-wide trends in criminal activity can be detected and addressed, experiences in one sector can be learned from, and a proactive technology driven program of fraud prevention can be resourced and utilised for the benefit of the whole payments industry and the wider community.

The first step to achieving such cohesion in Australia has recently been taken with the establishment of the joint ABA/APCA Fraud Direction Working Group. This Group will explore the potential for greater cooperation across the payments industry with the long term objective of developing a cooperative network, not just within the payments industry, but with government, law enforcement agencies and other payments system stakeholders. This will help ensure Australia's enviable record in payments fraud prevention is maintained.

**Stephen Halliday**  
Head of Industry Policy

**Arun Kendall**  
Research/Policy Analysis

**Caroline Pearce**  
Risk & Compliance

The ideas and opinions expressed in this article are those of the authors and not necessarily those of APCA or any APCA member. This article has been included in APCA's 2007 Annual Review for the purpose of promoting industry discussion on topical issues.