AN INDUSTRY APPROACH TO FRAUD PREVENTION
The Current State of Play

This paper has been prepared by the Industry Policy unit of APCA in response to a request by the Australian Payments Forum for the purpose of promoting discussion at the Forum. It does not represent the views of APCA, any member of APCA, the Australian Payments Forum or any participant in the Forum.

Table of Contents

1. Introduction

At the last meeting of the Card Payments Forum (now called the Australian Payments Forum), many participants expressed a view that fraud prevention was an important area of collaborative work for the Forum, and requested a special session of the Forum to discuss an industry-wide approach to fraud prevention, enhancing existing initiatives.

This follows an earlier industry seminar on fraud, the ABA/APCA Fraud Industry Directions Workshop held on Tuesday, 19 February 2008, in which attendees called for greater cross-industry cooperation on fighting fraud.

This paper provides an update on current fraud prevention initiatives by industry representative bodies and card schemes. It is not meant to be exhaustive: individual financial institutions undertake their own extensive fraud prevention programmes.

The focus of the paper is on industry-wide initiatives and does not look at the significant amount of work being undertaken by the regulators such as ASIC and the ACCC through bodies such as the Australasian Consumer Fraud Task Force and Scam Watch.

It is hoped that by providing this snapshot, participants at the Australian Payments Forum will be able to identify any gaps in the scope of fraud prevention activities and provide a useful starting point for discussion on whether there are any short-term and/or long term proposals which could further enhance the work currently being undertaken by the industry.

2. Global Initiatives

The following represent just some examples of cross-industry and governmental collaborative fraud prevention bodies that operate in other countries.

2.1. United Kingdom

2.1.1. CIFAS[1]

CIFAS enables Members to exchange details of applications for products, services or employment, which are considered to be fraudulent, because the information provided by the applicant fails verification checks.

[1] www.cifas.org.uk

Members can also exchange information about accounts and services which are being fraudulently misused or fraudulent insurance and other claims. CIFAS Members also exchange information about innocent victims of fraud to protect them from further fraud.

2.1.2. Dedicated Cheque and Plastic Crime Unit (DCPCU)[2]

The DCPCU is a special police unit fully sponsored by the industry through APACS. Its brief is to help stamp out organised card and cheque fraud across the UK.

2.1.3. Cardwatch[3]

Provides information about how card fraud takes place in the UK, what is being done to prevent it and how customers can prevent protect themselves.

2.1.4. Banksafe Online[4]

UK banking industry initiative to help banking users stay safe online.

2.1.5. Financial Fraud Action UK (APACS)

Financial Fraud Action UK is the name under which the financial services industry co-ordinates its activity on fraud, presenting a united front against financial fraud and its effects.

This new brand was launched on 6th July 2009 to replace the work carried out by APACS as the leading voice on fraud within the payments industry.

2.2. USA

2.2.1. The Identity Theft Assistance Centre (ITAC)[5]

The Identity Theft Assistance Centre (ITAC) is a not-for-profit industry collaborative initiative supported by about 50 major financial institutions in the USA. The ITAC's main focus is victim assistance but it also provides for information sharing amongst financial institutions and with law enforcement as well as public education and public policy engagement on identity theft.

2.2.2. National Cyber-Forensics and Training Alliance (NCFTA)[6]

The mission of the National Cyber-Forensics & Training Alliance (NCFTA) is to provide a neutral, collaborative venue where critical, confidential

[2] http://www.dcpcu.org.uk
[3] www.cardwatch.org.uk
[4] http://www.banksafeonline.org.uk
[5] www.identitytheftassistance.org
[6] http://www.ncfta.net/main/home/

information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia, and law enforcement. The Alliance facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations which are all intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

2.2.3. The President's Task Force on Identity Theft[7]

The President's Task Force on Identity Theft was established by Executive Order 13402 on May 10, 2006, as an element in the fight against identity theft. This body promotes a coordinated approach among government agencies to combat ID theft.

2.2.4. On-line advice and information sites[8]

These sites provide tips and advice for consumers to avoid fraud or to report fraudulent activities.

2.3. Ireland

2.3.1. Irish Fraud Bureau for Financial Crime[9]

The IFB is solely dedicated to the prevention of financial crime, providing a range of fraud prevention services to its members.

The bureau allows members to exchange information on financial crimes detected by their monitoring processes.

These crimes include credit card fraud, identity theft, loan fraud, or false insurance claims.

IFB members are able to swap details on innocent victims of fraud to protect them from further fraud. Consumers will have to give their consent for information to be used by the IFB.

Only members of the fraud bureau will be able to see warnings and they must be careful to establish the validity of any application for a product or service made from the address.

[7] http://www.idtheft.gov/about.html
[8] http://www.ftc.gov/bcp/edu/microsites/idtheft/
http://www.onguardonline.gov/#
http://www.fraud.org/
[9] http://www.ifb.ie/homepage/index.php

2.4. Canada

2.4.1. Fraud Prevention Forum[10]

The Fraud Prevention Forum is a group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organisations, who are committed to fighting fraud aimed at consumers and businesses. Through its partners, the Forum, which is chaired by the Competition Bureau, works to prevent Canadians from becoming victims of fraud by educating them on how to recognise fraudulent activities and report it to the right authorities.

2.4.2. Interac[11]

Interac Association raises public awareness about debit card protection and works closely with law enforcement and other partners to implement fraud prevention and education programs, such as the Protect Your PIN consumer awareness campaign, and Project Protect, a collaborative initiative focused on educating merchants about how they can help prevent payment card fraud.

2.5. South Africa

2.5.1. SABRIC[12]

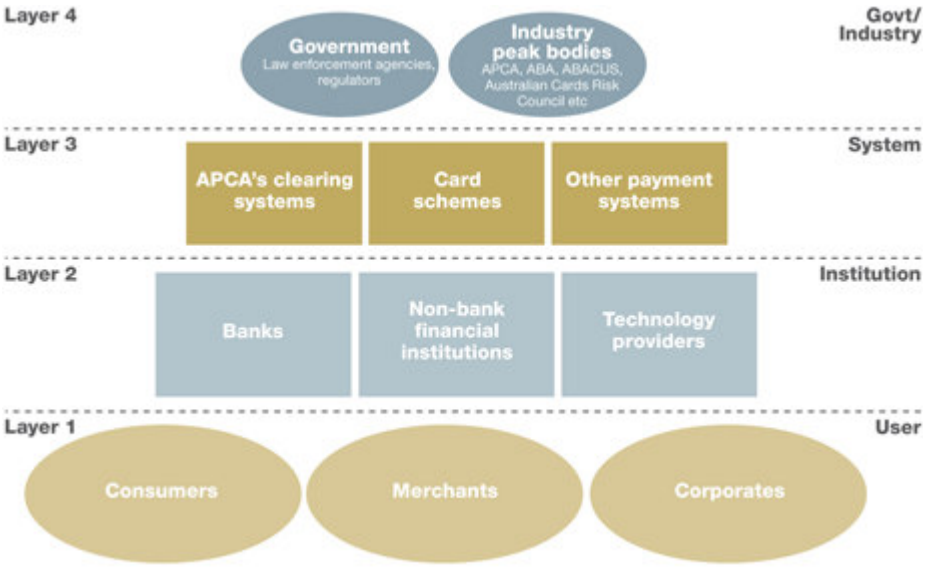
SABRIC is funded by four major South African banks and is tasked with providing:

- Crime intelligence (now referred to as Crime Risk Information);
- Risk management;
- Advisory services;
- Physical security of banking operations;
- National bank crime combating networks; and
- Management of banking crime related communication service.

3. Current fraud prevention initiatives in Australia

In previous work, APCA has referred to the four layers of fraud prevention as way of looking at how fraud prevention is approached in Australia[13].

[10] http://competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03110.html
[11] http://www.interac.ca/consumers/security_fraud.php
[12] www.sabric.co.za
[13] http://www.apca.com.au/AR2007/07_Fraud-prevention.htm



In this view, the argument was made that there was a great deal of work being done in the first three layers and more to be done at the fourth layer.

A great deal of work is undertaken by individual financial institutions to combat fraud, and card schemes in Australia have taken important steps to minimise card fraud. Below is a list of some of the measures undertaken across the industry which covers a range of initiatives at the third and fourth layers.

3.1. *ABA*

ABA fraud prevention activities generally fall into four broad categories, all of which are conducted in collaboration with member banks:

- Public policy
- Communication and education
- Standards and guidelines
- Operational coordination

The ABA works through a framework of industry working groups, led by the ABA Financial Crimes Steering Group and the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Focus Group.

Examples of industry initiatives follow.

3.1.1. Public policy

Over the last 12 months the ABA made submissions and engaged policy makers on matters including:

- Multiple AML/CTF legislation and rules changes (Australia and New Zealand)
- WA ID Crime Bill
- Commonwealth Cybercrime Inquiry
- E-Security National Agenda
- Victorian Law Reform Commission on surveillance
- Electronic verification (Cwealth AGD)
- International Trade Integrity Bill (Cwealth)

3.1.2. Communication and education

There is a significant investment in communication and education at industry level, which supports the activities of individual banks. ABA develops and maintains content on the main ABA site and a joint site, Protect Your Financial Identity, and conducts targeted campaigns on issues such as money mules.[14]

There is key focus on consistent industry messaging, for example (sample messaging on fraud):

- Banks have computer systems in place to constantly monitor transactions and if a transaction is identified as suspicious, it will be investigated to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction and the bank may take action to protect your account.
- Banks use a combination of safeguards to protect your information such as employee training, privacy policies, and security and encryption systems. Account holders are not liable for losses resulting from unauthorised transactions where it is clear that user has not contributed to the loss. There is usually an investigation by the bank to determine how the fraud has occurred.
- Banks are continuing to seek out security enhancements especially for online banking such as an on-screen keypad or a token which is designed to prevent the incidence of keystroke logging fraud by removing the need for a keyboard to enter in passwords.

3.1.3. Standards and guidelines

ABA and member banks have developed standards and guidelines to address specific needs. These include authentication and data compromise guidelines, and industry standards on accessibility of electronic banking. The

[14] *See: http://www.bankers.asn.au/Default.aspx?FolderID=128, http://www.protectfinancialid.org.au/ , http://www.bankers.asn.au/DONT-BE-A-MULE---SAY-NO-TO- TRANSFERRING-MONEY-FOR-CRIMINALS/default.aspx*

ABA also contributes to the development of other standards and guidelines such as the EFT Code.

3.1.4. Operational coordination

The central role of the ABA is policy work, but where needed the ABA plays a coordinating role on operational issues such as information sharing and crisis communication.

3.2. Abacus

Abacus is the industry body for the Australian mutual financial services sector, a strong alliance of mutual building societies, credit unions and friendly societies. The mutual sector has combined assets of some $75 billion, offering Australians a competitive alternative to banks and access to a range of savings products. Unlike banks, profits are not paid to external shareholders, but put back into better products and services for the over 5.5 million members (customers) and their communities.

Abacus has its own secure fraud portal with which it communicates with its 100 plus members on channels such as Card, Electronic and Lending fraud. Abacus is the aggregate dissemination point in real time for alerts, intelligence and advice including real time incident management - for example one of its larger mutuals has had not only protracted 'Phishing' attacks in past year but significant online card attacks. Abacus acts as first point of call to mitigate loss with the member organisation through specialised advice.

- Abacus each year runs a specialised program event for education of strategic and operational trends in financial crimes again across all fraud types not just Card fraud.
- Abacus has its own fraud committee comprised of Building Societies, large and medium sized mutuals where knowledge and depth of experience is shared and best practice for industry developed.
- Abacus has been providing wide ranging specialised fraud detection, prevention and loss mitigation services to mutuals since 2003 and being now owned directly by its members will continue this as a member service valued by industry as providing leadership in fraud and financial crimes knowledge and prevention services.

3.3. APCA

APCA's strategic focus is on improving the underlying payments system, including its security and safety. This includes a specific focus on fraud primarily in three ways:

- the collection and dissemination of payments fraud statistics;
- implementing industry initiatives to counter payments fraud; and
- providing a forum where fraud professionals can discuss areas of payments fraud

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. These statistics are collected from APCA's members plus the international card schemes.

APCA also collects monthly and quarterly statistics on cheque and debit card fraud for dissemination to its members.

The standards and guidelines around the different payments clearing systems include measures deliberately designed to reduce fraud. These include minimum security standards for PIN entry terminals, where APCA maintains an accreditation program for these terminals, minimum key management and encryption requirements for PIN protection and for protection of back-end systems, and minimum security requirements for cheques.

In addition, APCA has recently published new Merchant Guidelines for Terminal Security, which are designed to reduce the opportunities for terminal skimming.

The APCA Fraud Committee was originally established in mid-2001 to oversee fraud control, reduction and management measures in APCA's clearing systems. It was recently extended to cover fraud in payments systems in general and other related areas that are of interest to APCA's Members. Its objectives are:

- to share information on current fraud trends experienced by APCA's Members and methods for countering these trends; and
- to identify opportunities for industry cooperation in countering fraud, to assess these opportunities and support their implementation as required.

Membership includes banks, building societies, credit unions and major retailers who are self-acquirers.

Through the auspices of the Fraud Committee, APCA will shortly be launching a public PIN protection campaign.

APCA regularly liaises with other organisations, including card schemes, industry bodies, government and law-enforcement to facilitate co-operation in payments and payments-related fraud.

3.4. EPAL Pty

EFTPOS Payments Australia Limited (EPAL) is not yet fully operational. When it is it will undertake (at least) the following fraud prevention activities:

- Continuous review of technical standards and operational rules with the membership and other stakeholders,
- Information sharing with the membership, other providers and stakeholders and law enforcement,
- Pro-active engagement with law enforcement, and
- Continuous statistical analysis of Australia trends and monitoring of international developments,

These activities will be undertaken at a strategic level and at a tactical level in response to particular developments/incidents.

3.5. MasterCard

MasterCard Issuing Fraud Landscape

MasterCard's Issuing fraud basis points have reduced in 2009 in comparison with 2008 levels. Counterfeit fraud basis points steadily reduced and card not present fraud basis points remained constant.

MasterCard Acquiring Fraud Landscape

MasterCard's Acquiring fraud basis points have significantly reduced in comparison with 2008 levels. Counterfeit fraud basis points have experienced a large reduction and card not present fraud basis points have steadily reduced.

MasterCard Risk Mitigation Strategies

Counterfeit Fraud reduction has been driven by a holistic phased strategy that included introduction of EMV technology, Interchange Incentives and Interregional and Intraregional Liability shifts. This combined with tactical industry initiatives such as the creation of a Risk Tools Users Group ensuring all customers obtain the maximum benefit and efficiency from the detection systems have been the key elements in the reduction of this fraud type.

Card not present fraud remained constant and to manage this type of fraud in the future a holistic phased strategy has also been implemented that included introduction of SecureCode technology, Interchange Incentives and Interregional and Intraregional Liability shifts. This combined with tactical industry initiatives such as the creation of the MasterCard Online Security Taskforce driving SecureCode adoption amongst our customers and securing online payments have and will continue to be the key elements in the ongoing mitigation of this fraud type.

Card and Pin fraud has recently increased driven by terminal manipulation events in Australia. Whilst the majority of this fraud is perpetrated on

proprietary debit cards MasterCard created and chaired a Terminal Manipulation Taskforce taking the following actions to mitigate this risk:

- Distributed POS Security Best Practice Guides to acquirers and high risk merchants;
- Identification of high risk terminals and replacement strategies;
- High risk merchant briefings conducted in Sydney and Melbourne;
- Researched and communicated global best practice fraud detection strategies;
- High level industry briefings to the relevant stakeholders;
- Engagement of effected parties to implement tactical and strategic solutions;
- Engagement of technology vendors who have provided fraud prevention solutions;

MasterCard ensures the ongoing integrity of the card payment environment in Australia by driving visibility and fraud best practices in multiple industry forums. This also involves engaging members and sharing industry best practices through the quarterly Australian Cards Risk Council, PCI Working Group meetings and member fraud reviews. MasterCard also conducts monthly meetings with State and Federal police and the AHTCC to share information and intelligence and is involved in the development of new innovative risk products such as MasterCard Incontrol. This empowers the cardholders to directly manage controls and alerts on their card whilst allowing the issuer of the card to apply geographic controls to individual cards based on expected cardholder behaviour and fraud patterns.

3.6. Visa International

Globally, fraud within the Visa system has fallen to historically low levels, even while Visa card transaction volume has grown dramatically. However, although fraud in Australia is low by world standards, recent data indicates that payment card fraud in Australia is increasing. This trend is likely to continue as we see neighbouring countries implement enhanced security measures.

To counter this threat, Visa has developed a five-year agenda to strengthen payments security in Australia. The plan consists of seven key security initiatives with the aim to provide greater protection against fraud for cardholders, merchants and financial Institutions.

Key Initiatives:

- Moving to 100 percent chip card issuance. By 1 January 2010, banks and other financial institutions must issue all new Visa credit cards on chip; by 1 January 2011 all new Visa debit and reloadable prepaid

cards must be on chip; and by 1 April 2013, 100 percent of all Visa cards must be on chip.

- Ensuring all merchant acceptance terminals must be chip capable and activated by 1 April 2012
- Ensuring all new Automated Teller Machines (ATMs) commissioned must be chip capable by 1 January 2011.
- Introducing a broad rollout of PIN (Personal Identification Number) verification for all domestic transactions, with signatures no longer accepted from 1 April 2013.
- Issuers must enrol all Visa cards for Verified by Visa, a free service for cardholders that provides a password for secure online shopping, by 1 April 2012.
- All merchants who take online, telephone and mail order transactions must check the threedigit card verification code (known as CVV2) from 1 January 2011.
- Small and medium sized (Level 4) merchants will be required to implement higher levels of data security. Acquiring banks will be required to provide Visa with a program for their merchants to comply with the Payment Card Industry Data Security Standard (PCI DSS) by 30 April 2010 that includes a strategy for risk profiling, merchant education and compliance reporting twice per year.

3.7. Other Initiatives

3.7.1. Australasian Cards Risk Council

The Australasian Cards Risk Council (ACRC) is an advisory body whose purpose is to:

- Provide a forum to discuss Card risk issues affecting the industry;
- Consider best practices and risk management strategies; and
- Implement and monitor the effectiveness of any agreed plan or strategy.

The cards risk council members consist of the card schemes (Visa, MasterCard and American Express), issuers and acquirers in Australia and New Zealand.

The ACRC provides a forum to discuss and share crucial information relating to all aspects of card fraud. Members regularly share critical information about skimming devices and compromised card data to enable real-time responses, such as blocking compromised cards.

The ACRC has played an important role in allowing FIs to respond to the recent EFTPOS skimming frauds. It has been monitoring EFTPOS skimming both domestically and overseas for some time, with a focus on learning from those markets who have a more mature skimming

environment, for example Canada. In addition, the email alerts has provided the necessary information to be able to act quickly. The information sharing provided by the ACRC allows lessons to be learned quickly across issuers and acquirers and has resulted in reductions in the amount of money lost from such frauds.