Responding to organised payment card compromise and subsequent fraud

Brian Hay* and Julianne Webster**

Received (in revised form): 6th January, 2014

*Fraud and Cyber Crime Group, Queensland Police Service, Police Headquarters, GPO Box 1440, Brisbane, Qld 4001, Australia Tel: (+07) 3364 6622, Fax: (+07) 3364 6549, e-mail: hay.brianJ@police.qld.gov.au

**School of Criminology and Criminal Justice, Griffith University, Australia e-mail: j.webster@griffith.edu.au

Brian Hay is the head of Fraud and Cyber Crime Group, Queensland Police Service, Australia.

Julianna Webster is an Adjunct Research Fellow with the School of Criminology and Criminal Justice, Griffith University, Australia. Julianna is a criminologist with experience in criminal justice research, evaluation and public policy including policing responses to illicit drugs and cyber fraud.

ABSTRACT

The global endemic crime problem of payment card compromise and subsequent fraud continues to pose extreme challenges for the payments processing industry and for law enforcement. These challenges include developing strategies to minimise risk, including enhancing the security of cards for consumers, reducing loss for merchants and financial institutions, and enhancing intelligence sharing between industry and law enforcement. Case studies concerning the activities of transnational criminal networks responsible for card fraud show increasing levels of sophistication as well as the magnitude of financial loss. Correspondingly, the evidence suggests wide-ranging gaps in the design and implementation of equally sophisticated responses that can produce risk reduction and prevention. This paper draws on the problem-oriented policing, situational crime prevention and third-party policing theoretical approaches to propose a strengthened preventative response to the problem.

Keywords: intelligence; policing partnerships; fraud; crime prevention; payments

OVERVIEW

The primary aim of this paper is to discuss the transnational crime problem of counterfeit and card skimming. Drawing on recent statistics and law enforcement case studies, this paper highlights the challenges associated with policing these activities as well as reducing risk for consumers and for the payments processing industry. Combating the payment card problem with a set of responses requires consideration of crime theories as well technological and law enforcement capacity; while also considering the roles and responsibilities of the various industry and regulatory stakeholders. Recommendations for a strengthened approach to the problem are made in light of the inherent difficulties of policing this crime and for industry to curb its incidence. Recent experiences of policing partnership approaches that have focused on improving the flow of intelligence between third parties and law...
enforcement have shown promising crime reduction outcomes, such as precursor diversion prevention.\textsuperscript{1,2} This growing body of evidence highlights that harnessing third parties in a proactive capacity shifts the focus from a predominantly reactive enforcement model to an approach that targets crime reduction at key access points to mobilise targeted guardianship practices. The analysis of the problem suggests that, as well as mobilising partnerships, proactive intelligence sharing between industry and law enforcement can facilitate improved early warning processes. These systems can improve the capacity for transnational law enforcement to respond, prevent, detect and prosecute offenders. Additionally, the proactive monitoring of third-party data, such as credit histories, provides more early warning opportunities, which impact on prevention and early detection of victimisation. The strengthened proactive partnership approach discussed in this paper incorporates the card industry implementing situational measures to reduce risk of fraud, formalising partnerships between business and law enforcement to improve the capacity and flow of meaningful intelligence, and law enforcement developing transnational early warning notifications to alert countries to the constantly evolving trends in fraud offences. Central to these approaches is the need for industry and law enforcement to shift away from the traditional localised jurisdictional view of the problem to a perspective that understands and conceptualises the problem and its solution/s in a transnational multi-agency response framework.

**FRAUD INCIDENCE: THE SIZE OF THE PROBLEM**

The global endemic crime problem of payment card compromise continues to pose extreme challenges for the payments processing industry and for law enforcement. The extent of the problem continues to grow annually as criminal networks expand their reach and continue to increase the sophistication of their methods.

In 2012, there were over one and a quarter million transactions involving credit, debit and charge card fraud against Australian cards, making a total loss of over A$260m. Interestingly, the majority of losses for non-proprietary cards occurred in overseas counties: 679,390 transactions or almost A$134m (see Table 1). These data alone reflect the strong transnational nature of organised crime efforts specifically against the card industry. The other interesting note is that of the ‘Scheme’ cards, 81 per cent of the fraudulent transactions were card not present (CNP). These data confirm the strong link between card fraud and transnational criminal efforts.

Between 2006 and 2012, fraud incidents, including those involving lost and/or stolen cards, cards never received, fraudulent application of cards, counterfeit and/or skimming of cards as well as fraud involving CNP in Australia continued to increase exponentially, with an overall increase of 291 per cent in seven years. Similarly, other countries experienced rates of growth in card fraud incidents, albeit much higher, recording a 520 per cent increase over the same period. Apart from a small decrease in the value of frauds in Australia between 2008 and 2009, the increase in the cost of fraud is significant, and has not abated in Australia or worldwide in recent years (see Figures 1 and 2). In Australia, there were over 1.84 million card-related fraud incidents during the period, with an associated cost of over A$512m (see Table 2 and Figures 1 and 2).

Figure 2 depicts the protracted growth of this crime problem over time in Australian and overseas jurisdictions. In
2011 and 2012, an average loss of A$423,435 was reported every day worldwide. Of this, A$296,505 was perpetrated in Australia every day.

The extent of payment card fraud is very difficult to ascertain, owing to data unreliability and selective reporting. Law enforcement personnel working in Australian fraud squads agree that the Australian banking community is reticent to reveal the full extent of the card fraud problem. Limited disclosure of fraud by banks has been experienced on numerous occasions: for example, when law enforcement agencies are not advised of card skimming attacks on automatic teller machines (ATMs). Commonly, law enforcers are notified of a skimming device when a member of the public reports it, not as a matter of practice by the financial institution. Other means to identify the size of the problem are through surveys and police-recorded crime. In 2012, a survey of 13,000 people across 24 countries conducted by Norton, found 72 per cent of respondents had been a victim of cybercrime with an estimated direct cost of these cybercrimes at US$110bn for the preceding 12 month period.\(^3\)\(^4\)

Activities included in the definition of

---

### Table 1: Card related fraud incidents in overseas countries

<table>
<thead>
<tr>
<th>Category</th>
<th>Transactions</th>
<th>Value ($)</th>
<th>Transactions</th>
<th>Value ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost/stolen</td>
<td>83,636</td>
<td>14,414,354</td>
<td>21,889</td>
<td>8,318,853</td>
</tr>
<tr>
<td>Never received</td>
<td>25,262</td>
<td>6,780,682</td>
<td>1,185</td>
<td>446,470</td>
</tr>
<tr>
<td>Fraudulent application</td>
<td>5,185</td>
<td>3,409,868</td>
<td>274</td>
<td>93,059</td>
</tr>
<tr>
<td>Counterfeit/skimming</td>
<td>37,484</td>
<td>13,047,707</td>
<td>45,035</td>
<td>14,602,763</td>
</tr>
<tr>
<td>Card not present (CNP)</td>
<td>360,221</td>
<td>72,645,147</td>
<td>609,655</td>
<td>110,155,844</td>
</tr>
<tr>
<td>Other</td>
<td>3,016</td>
<td>714,014</td>
<td>1,352</td>
<td>355,619</td>
</tr>
<tr>
<td>Total</td>
<td>514,804</td>
<td>111,011,772</td>
<td>679,390</td>
<td>133,972,608</td>
</tr>
</tbody>
</table>

Source: Australian Payments Clearing Association (APCA) 2013.

### Table 2: Card related fraud incidents in Australia between 2008 and 2009

<table>
<thead>
<tr>
<th>Category</th>
<th>Transactions value ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debit card fraud — PIN used</td>
<td></td>
</tr>
<tr>
<td>Lost/stolen</td>
<td>18,452</td>
</tr>
<tr>
<td>Never received</td>
<td>3,057</td>
</tr>
<tr>
<td>Counterfeit/skimming</td>
<td>21,638</td>
</tr>
<tr>
<td>Other</td>
<td>1,328</td>
</tr>
<tr>
<td>PIN used total</td>
<td>44,475</td>
</tr>
<tr>
<td>Debit card fraud — PIN not used</td>
<td></td>
</tr>
<tr>
<td>Lost/stolen</td>
<td>58</td>
</tr>
<tr>
<td>Never received</td>
<td>2</td>
</tr>
<tr>
<td>Counterfeit/skimming</td>
<td>37</td>
</tr>
<tr>
<td>Other</td>
<td>15</td>
</tr>
<tr>
<td>PIN used total</td>
<td>112</td>
</tr>
<tr>
<td>Total debit card fraud</td>
<td>44,587</td>
</tr>
</tbody>
</table>

Source: Australian Payments Clearing Association (APCA) 2013.
cybercrime were viruses, online credit fraud, unsolicited pornography, phishing and receiving excessive spam. The costs of fraud are significant, and available estimates are likely to underestimate substantially the real total costs. In 2011, the Australian Bureau of Statistics estimated at least 1.2 million Australians experienced at least one fraud incident in the 2010–11 financial year; with an associated total loss of A$1.4bn. The 2011 estimate was up from 806,000 victims (15 years and over) experiencing at least one person fraud offence in 2007. The loss estimate incorporates only the direct loss to the victim and excludes other costs, such as those incurred by banks and businesses associated with investigation and reimbursement, law enforcement investigation, opportunity costs for victims associated with time for reporting and funds recovery, as well as less tangible costs such as

---

**Figure 1** Number of frauds: credit, debit and charge card perpetrated in Australia and overseas on Australia-issued cards, 2006–2012

**Figure 2** Value of frauds — credit, debit and charge card perpetrated in Australia and overseas on Australia-issued cards, 2006–2012

---

*Source: Australian Payments Clearing Association (APCA) 2013*
psychological harm and associated impacts to families and communities.\textsuperscript{6,7} In Australia, police-recorded crime for fraud offences between 2002 and 2012 shows increases in every jurisdiction over this period, with the exception of Queensland and Tasmania (see Table 3). Reported incidents of fraud offences since 2003 show an average of 73,413 offences per year in Australia, or an average of 1,411 offences per week.

But it is known that, in 2012, there were one and a quarter million transactions involving credit, debit and charge card fraud against Australian cards. Therefore there is a significant ‘dark figure’ (the difference between incidence and reporting) for card fraud. One of the major factors affecting levels of official reporting of fraud to police is the standard practice employed by financial institutions to investigate and ‘clear’ fraud cases involving their customers. While this is likely to be viewed as good business practice, it creates little incentive for victims to report the crime to police. Crime underreporting affects governments’ priorities and capacity to make accurate and/or timely decisions about the course of action to be employed to address problems. While Figure 3 indicates that reported incidences of fraud are reasonably steady since mid-2000, the APCA data suggest that the problem is growing exponentially (see Figures 1 and 2).

To devise appropriate responses to the problem, it is important to understand how cards are compromised and the composition of the criminal networks engaging in these activities. The most common methods for compromising cards are through card skimming, lost/stolen, hacking of databases, key logging malware, internal data breaches, point of sale (POS) terminal compromise, as well as phishing and phone scams. All these methods are technology based. In response, a number of technology-based security aids have been implemented to reduce card vulnerability to fraud. Mandatory chip and pin technology was introduced in the UK in February 2006. The new technology resulted in a mass upgrade to cards (42 million) as well as to POS terminals (850,000) and ATMs (40,000 ATMs).\textsuperscript{8,9} The impact on fraud from the introduc-

<table>
<thead>
<tr>
<th>Year</th>
<th>Queensland</th>
<th>New South Wales</th>
<th>Victoria*</th>
<th>South Australia*</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Western Australia</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011–2012</td>
<td>14,916</td>
<td>38,145</td>
<td>22,773</td>
<td>2,352</td>
<td>427</td>
<td>249</td>
<td>13,726</td>
<td>92,588</td>
</tr>
<tr>
<td>2010–2011</td>
<td>16,600</td>
<td>36,276</td>
<td>19,895</td>
<td>2,866</td>
<td>498</td>
<td>235</td>
<td>8,106</td>
<td>84,476</td>
</tr>
<tr>
<td>2009–2010</td>
<td>18,182</td>
<td>36,491</td>
<td>19,979</td>
<td>3,012</td>
<td>472</td>
<td>276</td>
<td>9,231</td>
<td>87,261</td>
</tr>
<tr>
<td>2008–2009</td>
<td>17,857</td>
<td>37,111</td>
<td>23,016</td>
<td>2,846</td>
<td>547</td>
<td>n/a</td>
<td>11,140</td>
<td>92,517</td>
</tr>
<tr>
<td>2007–2008</td>
<td>19,091</td>
<td>37,134</td>
<td>23,632</td>
<td>3,261</td>
<td>688</td>
<td>n/a</td>
<td>9,564</td>
<td>93,370</td>
</tr>
<tr>
<td>2006–2007</td>
<td>22,955</td>
<td>33,002</td>
<td>25,856</td>
<td>3,956</td>
<td>596</td>
<td>n/a</td>
<td>9,241</td>
<td>95,606</td>
</tr>
<tr>
<td>2005–2006</td>
<td>25,015</td>
<td>35,241</td>
<td>27,689</td>
<td>3,970</td>
<td>1,101</td>
<td>n/a</td>
<td>9,979</td>
<td>102,995</td>
</tr>
<tr>
<td>2004–2005</td>
<td>25,885</td>
<td>33,625</td>
<td>27,630</td>
<td>3,684</td>
<td>1,496</td>
<td>n/a</td>
<td>6,906</td>
<td>99,226</td>
</tr>
<tr>
<td>2003–2004</td>
<td>25,522</td>
<td>30,070</td>
<td>30,201</td>
<td>4,914</td>
<td>1,415</td>
<td>n/a</td>
<td>5,704</td>
<td>97,826</td>
</tr>
<tr>
<td>2002–2003</td>
<td>30,063</td>
<td>33,148</td>
<td>30,213</td>
<td>5,756</td>
<td>1,745</td>
<td>n/a</td>
<td>7,123</td>
<td>108,048</td>
</tr>
</tbody>
</table>

*Broader offence grouping of deception. n/a — not available.
Source: Queensland Police Annual Statistical Review; BOCSAR NSW recorded crime quarterly reports; Tasmanian Crime Reports; Northern Territory Tri-service report — Police; Fire and Emergency Services; Tasmanian Department of Police and Emergency; Management Annual Reports; OCSAR (WA); Victorian Offences recorded by Offence Code 2002–03–2011/12 and South Australian Police Annual Reports.
tion of tougher technological measures was examined by Finch, who interviewed 19 fraudsters in 2004 and again in 2009. The study found that chip and pin technology increased the difficulty for fraudsters, as they needed to have both elements to use cards fraudulently. Finch, however, found that chip and pin technology discouraged only around 20 per cent from further illegal activities. Many of these individuals had less than five years’ fraud experience and stated that they were unwilling to adopt new methods to continue. Finch found that the fraudsters’ perceived heightened risk of detection was a significant deterrent, particularly to individuals who were ‘less entrenched’ in the activity. For the deterred fraudsters, Clarke’s situational crime prevention theory fits neatly, with fraudsters weighing up costs versus benefits of engaging in the crime. Those criminals who assess the costs and/or risks to outweigh the potential benefits are deterred from the behaviour.

This study, however, found that not all fraudsters were deterred as a result of tightening up or target hardening. The remainder, who were not deterred, viewed the new environment as simply a new game with new rules to learn and overcome. The study showed that standalone changes to technology did not make a wholesale impact on motivation to offend. In addition, more entrenched fraudsters may be savvier to the realities of law enforcement investigations and prosecutions, and hence consider the heightened risk still to be a low risk.

Observations made by the first author indicate that criminal networks appear to understand, to a degree, the complexity faced by law enforcement to initiate international fraud investigations successfully and to prosecute. One of the major barriers is effective communication between countries, including significant language and cultural barriers as well as inconsistent legislation. Low rates of reporting also
reduce police opportunity to be aware of crimes and/or investigate offenders. In these circumstances, there is little to deter criminal groups from continuing to engage in card fraud when investigations are limited, and barriers to successful prosecution are high. The analysis of the data, together with substantial experiential knowledge, confirms that criminal networks use the enormous borderless potential of the internet to commit transnational crimes that largely go unreported and are extremely difficult to investigate and prosecute. Together with these barriers, the increasing sophistication of criminal groups also increases the challenges for banks, businesses, individuals and law enforcement.

**TRANSNATIONAL CASE STUDIES**

Case studies illustrating the increasing sophistication of transnational criminal networks responsible for card fraud show that there are three fundamental phases of criminal operation in respect of cards.

The first phase is the acquisition of the card data. Recent examples in Australia include Romanian ATM card skimming gangs. These gangs were found to be entering the country in one capital city and, during the course of two to three weeks, they travelled through the major cities and harvested skimmed card details during their stay, before departing from a different international airport.

A second example involved a Romanian-based cybercriminal syndicate who committed a large data theft operation involving 500,000 Australian credit cards. This data theft enabled thousands of fraudulent transactions to be carried out in numerous overseas locations, including Europe, Hong Kong, Australia and the USA.

The second phase in the operation of the transnational crime fraud market is the trading of the data. The most common place for this to occur is in the ‘dark market’ — the deep web where cyber criminals openly trade in illicit commodities, including credit card data. A joint operation between the Fraud and Cyber Crime Group of the Queensland Police Service and the US Secret Service targeted a Malaysian national operating a counterfeit card production business in the ‘dark market’. During the investigation over a two-week period, 87 suspects were identified in 21 countries. The case illustrates the potential for transnational criminal groups to operate and flourish across numerous countries with the assistance of the internet. The case also demonstrates the capability for Australian law enforcement to work successfully transnationally.

The third phase is cash extraction and/or fraudulent transactions. This is the phase where the compromised card data are used to commit fraud. In April 2013, transnational criminal organised networks made 40,500 transactions over ten hours in 27 countries to extract around A$45m from compromised card accounts.

These case studies highlight the three main elements of card fraud and highlight the high level of organisation and sophistication of these groups, as well as the swiftness with which card fraud is committed. As shown by Finch, highly organised and highly sophisticated transnational crime groups are unlikely to be deterred from engaging in these activities when the rewards are significant and the risk of apprehension and prosecution is perceived as relatively low. Linked-up and collaborative system-wide and community-wide changes that focus on optimal risk reduction and prevention strategies are required, as simply tweaking the system will have only a small impact on the illegal activities of criminal groups who are less entrenched and sophisticated.
CURRENT RESPONSES TO CYBER FRAUD

Internationally, numerous governments have devised strategies to respond effectively to the growing threat of cybercrime. In 2010, the UK released its ‘Cyber Crime Strategy’ and, in 2011, the USA released its ‘Strategy to Combat Transnational Organised Crime: Addressing Converging’. Similarly, the Australian Government aspires to cyber security through a national strategy encompassing seven key strategic priorities. These are to have a greater awareness of threats to government and key infrastructure, and, in doing so, improve the capacity to detect, analyse and mitigate cyber threats. The second priority is to educate all Australians through the provision of practical knowledge and tools, which assists all individuals to protect themselves online. This is followed by a strategy to forge closer partnerships between business and government to enhance cyber security, with particular attention to infrastructure, networks and products and services. The intention of the strategy is for government systems to model best practice in securing government transaction systems. Next is a commitment to international engagement, which promotes and supports Australia’s national interests in cyber security. Priority six has a specific focus on legal and law enforcement elements of cyber security, specifically to ensure the provision of an effective legal framework that supports enforcement capabilities in the targeting and prosecution of cybercriminals. The ongoing development of knowledge, skills and innovation through investment in building a skilled cyber security workforce is the final priority. While these broad objectives are largely top-down, building capacity in business to enhance cyber security is a strategy that requires business and industry to prioritise investment and commitment in this regard. A distinct gap in the literature is how businesses develop mitigation strategies against external fraud. Typically, the focus of fraud deterrence research is how businesses can mitigate against rogue employees’ actions to defraud. Business vigilance in both internal and external fraud contexts, however, are equally important for reducing vulnerabilities in financial transactions and for the card industry more broadly.

In the banking environment, these businesses have fiduciary responsibilities to their customers. A fiduciary relationship is where a person (the fiduciary) undertakes to act for another (the principal), and in doing so, the fiduciary must place the principal’s interests ahead of its own. The Payments System Board (PSB), within the Reserve Bank of Australia, have regulatory jurisdiction in Australia for the payments processing industry. The Australian regulator, however, has been described as having a ‘light touch’ approach, whereby its preferred means for communicating standards to industry is through consultation and policy development. Since 1998, the PSB’s regulatory ‘intervention’ record has been minimal — consisting of just a few cases, while the PSB provides policy guidelines for the Australian payments processing industry around a broad range of processing mechanics: for example, credit card surcharges and how to process a dishonoured cheque; policies that specifically reduce consumer vulnerability to fraud are unspecified.

The fiduciary relationship is one of trust, and obligates the fiduciary to act with the best interests of the person in mind. Simply put, financial institutions and payments processing merchants are responsible for acting in the best interests of the customer with whom there is a fiduciary obligation. In Australia, this obligation is proscriptive, meaning that the fiduciary must not act in certain ways,
including: avoiding a position of conflict of duties regarding the principal; and not acting for their sole benefit — or that of third parties — without the consent of the principal. While not implicitly stated, Australia’s proscriptive standard on fiduciary obligations could also be construed to mean that these third parties must not act in a deliberate way that disadvantages the principal. In other words, technologies and processes to reduce the risk of card fraud — as well as partnership strategies between banks, businesses, the card industry and government agencies such as law enforcement — should not be held back on the basis of enhancing business profitability. Reducing vulnerability to card fraud is a fiduciary responsibility, and developing a more collaborative and proactive response should be a higher priority for the payments processing industry worldwide. It is also the responsibility of the fiduciary to protect the identity of the client whose account has been compromised. Law enforcement experience suggests that financial institutions, who do not cancel cards immediately, increase the opportunity for criminals to take over the card holder’s identity. This inaction further exposes the person to further fraud victimisation, and can be prevented.

Police have the fundamental responsibility to protect life and property and, prior to the emergence of the internet, policing was focused at the ‘local’ level. In this environment, detectives were accustomed to conducting investigations and making arrests. In a localised crime market, police careers were established on the quality and quantity of arrests. The global crime environment, however, driven by transnational crime elements, has changed the nature of police work and created significant challenges. These include police not being able immediately to locate the offender and to prosecute accordingly, and the subsequent willingness of victims to be forthcoming with information in the remote likelihood of apprehension. Similarly, police have limited access to information that could assist their investigations and/or prevention activities. In the context of cybercrime, the challenges are exacerbated by the sophistication of transnational groups who operate and proliferate in the ‘dark market’. Law enforcement efforts are hampered owing to substantial underreporting, and this is directly influenced by businesses subsuming fraud as a cost of doing business. The available data show that fraud is continuing to grow considerably, and the collective response to fraud is not keeping pace. It is clear that a strengthened approach that involves key stakeholders is required.

CONCEPTUALISING A STRENGTHENED APPROACH

In Australia, work has commenced to strengthen the security mechanisms available to governments, business and customers operating in cyber environments. To date, however, these responses have not specifically addressed the weaknesses in the law-enforcement toolkit to make a tangible impact on this crime. This response includes capacity to employ innovative proactive preventative measures that are heavily data reliant and data driven. Implementing strengthened responses includes strategies to improve overall card security as well as improve partnerships, intelligence sharing and early warning processes.

A situational crime prevention approach encourages police and others to examine the context of the crime and to seek to design and implement measures that can counter an identified crime occurring at a particular place or context. Similarly, problem-oriented policing encourages police to analyse the
activities of offenders in the commission of crime and to develop strategies to counter these opportunities, to increase offenders’ risk of detection and to make crime less attractive in these contexts.\textsuperscript{24} The third-party policing approach stems from these two approaches, whereby, place managers and guardians are identified and mobilised to assist law enforcement, often through the use of existing regulation, to provide a consistent crime control or prevention response to an identified problem.\textsuperscript{25} The problem of counterfeit cards and card skimming provides opportunities for situational measures, problem-oriented measures and third-party measures to strengthen prevention, increase prosecution and reduce risk of victimisation.

Figure 4 illustrates how police can mobilise guardianship through a third-party policing model. First, it shows police identifying the access points with which to design and implement responses. These access points are points where certain crimes are enabled, simply by the nature of their legitimate business operations.\textsuperscript{26} Secondly, the model shows how the mobilisation of third parties through regulations both co-opts and empowers that third party to perform specific crime prevention or control roles.\textsuperscript{27} Lastly, the outcome of police engagement with third parties, through this model, is the consistent implementation of strategies designed to reduce and prevent crime. The nature of the model, as a collaborative partnership — which typically involves information sharing — also increases the risk of apprehension, and therefore opportunities to influence offender decision making and deterrence.\textsuperscript{28}

Conceptually, third-party policing can be viewed as the umbrella strategy that enables consistent and committed partnerships between and across governments, banks and businesses. Within this broader strategy, problem-oriented and situational crime prevention responses are useful frameworks for devising target-hardening strategies to ever-changing card security vulnerabilities.\textsuperscript{30}

Changing the appearance of cards is a
situational response, which can and is frequency circumvented by criminal groups. The functionality of the card, however, is an area that can be controlled and modified to make card fraud more difficult. Problem-oriented measures include making the card more difficult to compromise by using mandatory chips and implementing additional controls around use of the card: for example, making the use of a personal identification number (PIN) for every transaction mandatory. Card issuers can control the functionality of the cards and can implement increased security measures, which can collectively result in fraud prevention.

As illustrated in Table 1, a large proportion of offences involving Australian cards are perpetrated overseas. A problem-oriented approach seeks to minimise crime at a particular place or context. Thus, a geographically limited card would automatically reduce a large quantity of overseas perpetrated frauds. As is typically the case with a number of Australian banks and financial institutions, unusual card use in overseas jurisdictions is rapidly flagged and verified with the cardholder. Cards are stopped or cancelled when suspicious activity is detected. This model is reactive, however: the fraud has already taken place, and a financial loss has already been incurred. A card designed specifically for use on the internet may also be an approach that minimises risk of fraud for merchants and customers, as is the requirement that all card use is dependent on the accurate use of a PIN. A prevention model that incorporates these elements seeks to minimise risk, disruption and loss, and thereby requires third parties to implement situational measures with technology, which effectively facilitate these measures.

There is also an opportunity to do more with respect to creating more consistent and reliable early warning capacity across financial institutions and with law enforcement. A third-party policing response that is mobilised through regulations could be used to create consistency and processes to facilitate the rapid sharing of information about fraud trends. The timely sharing of this information assists countries to analyse and develop mitigation strategies to circumvent the otherwise full impact of a new crime trend. Intelligence sharing from financial institutions to law enforcement is one of the key pillars of enhancing early warning capacity and being better prepared for the ongoing influx of new criminal schemes that circulate the globe. Building capacity in law enforcement to receive and analyse increased levels of intelligence for strategic as well as operational purposes also needs to be considered.

As part of the enhanced early warning intelligence sharing, a bank-funded credit rating monitoring system would appear to be another important and logical component to facilitate the early detection of fraudulent activity that encompasses card and identity fraud more broadly. This is an example of existing information being used more strategically by industry and law enforcement to detect fraud patterns and provide more targeted opportunities to reduce risk and loss to business and individuals.

For victims of fraud by counterfeit or card skimming, it is also pertinent that identity restoration practices are expedited and that victims are afforded support from governments and financial institutions in this process. Once more, a better coordinated and ‘joined-up’ response in this regard is likely to lessen the impact on victims.

CONCLUSION
Understanding of the magnitude of the counterfeit and card skimming problem is
Hampered by the availability of accurate information that is publically accessible. But it is known, from victim surveys that the rate of fraud victimisation is consistently much higher than that reported to police. The fraud ‘dark figure’ significantly impedes one’s ability to ascertain precisely the nature of counterfeit and card skimming in Australia and/or worldwide. This paper has highlighted the need for a change of approach, one that no longer accepts the cost of fraud as a consequence of doing business, to a position that seeks to address the very significant problem — with an increased focus and investment in prevention activities, including situational measures, partnerships and intelligence sharing facilitated through third-party policing frameworks. Table 4 summarises the recommended strategies discussed in this paper, along with the agencies to be involved in championing change. While it is not possible to estimate costs associated with these approaches, it is the authors’ assessment that many of the strategies involve activities that are already occurring. What is missing in the framework is the joined up partnership that enables value adding that can significant benefit others to reduce risk, reduce loss and protect consumers better.

It is difficult for any one industry to stay ahead of the fraud curve, therefore genuine innovation, partnerships and collaborations across and between government, industry and law enforcement agencies are necessary to affect meaningful change. It is clear that there is an opportunity to do more, and that better prevention and partnership initiatives play a key role in the response into the future. Fraud should not be accepted as an expense, but rather as a significant problem that, with innovation, partnerships and intelligence, is something that can be better controlled and reduced.

**Authors’ Note**
The views expressed are the authors’ own.

**References and Notes**


[6] Ibid.


[12] Ibid.


[14] Finch, ref. 10 above.

[15] Ibid.


[22] Australian Government, ref. 16 above.

[23] Clarke, ref. 13 above.


[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.
