Chapter 6
Technology and identity crimes

6.1 Having examined the regulatory relationships between the private and public sector, together with some crime prevention tools and strategies, the committee now examines the increasing use of technology in financial related crime, together with the increasing incidents of identity crime.

6.2 This chapter examines some of the technological enablers of financial related crime, including the 'Darknet', alternative currencies and the roll out of 'tap and go' technology.

6.3 This chapter also examines the role of iDcare as the lead organisation responsible for providing assistance to victims of identity crime.

6.4 Identity crime and credit card fraud are also examined in the context of new technology. Law enforcement strategies for addressing identity theft, especially the Document Verification System (DVS) are also examined in this chapter.

Technology

6.5 Many submitters and witnesses discussed the significant role that technology plays in facilitating financial related crimes. While technology has always been used for nefarious purposes, many witnesses and submitters emphasised the increasing sophistication of criminals and their reliance on rapidly changing technology.

6.6 The ACC submitted that financial crime is becoming significantly more sophisticated, in large part due to advances in technology. The increased use of technology by financial service users is playing a decisive role in facilitating financial related crime.[1]

6.7 The ACC argued that in the international space, three factors shape the serious and organised crime environment:

> …the infinitely complex, diverse and pervasive nature of serious and organised crime which is fundamentally enabled by globalisation, technology and cyber capabilities...[2]

6.8 The AFP emphasised its concerns with respect to the threat of cybercrime, where financial related crimes are perpetrated against individuals or corporations. The AFP argued that new technologies were allowing organised crime organisations to facilitate advanced and complex criminal acts against Australian interests:

---

1 Mr Chris Dawson APM, Chief Executive Office, Australian Crime Commission, *Committee Hansard*, 10 September 2014, p. 1.

2 ACC, *Submission 5*, p. 7.

> Cybercrime that is undertaken for financial gain is a significant issue for Australia as it is complex, multi-jurisdictional and is generally considered an enabler for financial crime. [3]

6.9 Submitters also raised the increasing use of specific technological tools in financial related crime, like Bitcoin and Darknet, both of which are examined below.

Bitcoin

6.10 Bitcoin is a virtual currency which allows online payments via peer-to-peer transfers between computers, into 'real currency' and provides users with an alternative to traditional banks. Bitcoin transfers are made by online exchange houses that facilitate exchanges between virtual currencies and standard currency.[4] The ACC noted that peer-to-peer transfers of virtual currencies can occur instantaneously without the need for transfers via third parties:

> This offers an entirely legitimate means of transferring value outside of the formal finance sector.
>
> The anonymity that this process affords, and the ease with which virtual currencies can be exchanged within and across borders, make them attractive to serious and organised crime. Virtual currencies are also attractive to individuals seeking to engage in criminal activities and the 'darknet', such as the former Silk Road, which relied solely on Bitcoin for the trade in illicit goods, including illicit drugs.[5]

6.11 The AFP submitted that the increased popularity of online currencies like Bitcoin provides additional opportunities for criminals to hide their identities online due to the lack of regulatory oversight of online currencies.

6.12 The ACC explained that the extent of Bitcoin's use for criminal activities is as yet an unknown quantity:

> Although virtual currencies such as Bitcoin are seen as vulnerable for exploitation by organised crime seeking to facilitate money laundering activities, evidence that this is occurring on a large scale is yet to be identified.[6]

6.13 AUSTRAC submitted that the evolution of digital currencies allowed internet based means of transferring 'real-world values' in lieu of using traditional currencies or physical commodities. AUSTRAC noted that digital currencies allowed individuals and entities to conduct both simple and complex international funds transfers outside standard regulatory arrangements:

> The evolution of digital currencies has led to the development of internet-based, electronic means of transferring ‘real-world’ value. In contrast to traditional physical currencies issued by national governments, digital

3 AFP, *Submission 6*, p. 7

4 ACC, *Submission 5*, Attachment 1, p. 17.

5 ACC, *Submission 5*, Attachment 1, p. 17.

6 ACC, *Submission 5*, Attachment 1, p. 18.

> currencies (such as Bitcoins, SolidCoins and Linden dollars) are issued by commercial enterprises and are not backed by traditional currencies, precious metals or other physical commodities.
>
> Digital currencies potentially allow individuals and entities to conduct quick and complex international funds transfers outside the regulatory requirements of the traditional financial system. Digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act.[7]

6.14 AUSTRAC noted that the anonymous nature of digital currencies may appeal to criminal individuals or groups, who may see the currency as an instrument with which to evade tax or to obscure the origin of illicitly obtained funds:

> Criminal groups and individuals may increasingly use digital currencies, as opposed to online trading of real currency, due to the anonymity. These digital currencies present challenges for government agencies in following the money trail.[8]

6.15 The AFP agreed with the premise that the lack of AUSTRAC oversight of Bitcoin means it is an attractive method for money laundering or tax evasion in Australia:

> ...the use of these currencies may circumvent Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting requirements regarding the movement of monies into, and out of, Australia.[9]

6.16 The ABA also noted in its submission the increasing availability of Bitcoin as an alternative currency. The submission noted the US Inland Revenue Service recognised Bitcoin as a currency and that it had been seized as part of their confiscations of the proceeds of crime program.[10]

Darknet

6.17 As outlined above, Darknet is often associated with the use of Bitcoin to enable financial related crime, including the use of stolen or misappropriated funds to purchase illicit goods or services.

6.18 SAPOL noted that with an 'onion router', an internet user could obtain access to the Darknet where they could access a variety of illicit material, including child exploitation sites or online drug markets:

> These darknet sites are predominantly around child exploitation material. There are drug sites. They had identified their own drug sites. It is a bit like Gumtree—you put an order in, say what you want, you give an address and then it will be sent to you. But because of the way the site operates, it uses your IP address because it comes through what is known as the onion

7 AUSTRAC, Submission 10, p. 20.

8 AUSTRAC, Submission 10, p. 20.

9 AFP, *Submission 6*, p. 7.

10 ABA, *Submission 4*, p. 5.

> router. There is no way of identifying who the person is. Because it comes in through that piece of software, the actual identity is stopped.[11]

6.19 While law enforcement agencies can act to some extent against Darknet sites, SAPOL noted that it was difficult for law enforcement to keep track of purchasers and sellers of illicit substances through the internet and Darknet.[12]

6.20 Victoria Police agreed that Darknet was an issue, as it facilitated criminal access to firearms sales, drugs and child exploitation materials.[13]

Committee view

6.21 The committee shares the concerns of Commonwealth, state and territory law enforcement agencies about the use of Bitcoin to procure illicit products and services on the Darknet.

6.22 The committee believes it is critical to ensure that Australian federal law enforcement agencies have adequate strategies and tools for the detection and disruption of technologically enabled financial crime.

6.23 However, at the time of writing the committee notes the Senate Economics References Committee is currently undertaking an inquiry into digital currency. This inquiry, which is focussed in detail on the implications of the emergence of virtual currencies, was extended on 2 March 2015 to report on 10 August 2015.[14] Accordingly, the committee has decided not to make any specific recommendations in this regard, but will await the conclusion of that inquiry process.

Identity crime

6.24 The committee heard from numerous submitters about increasing incidents of identity crime in Australia. Identity crime takes many forms, including using a fabricated or stolen identity to commit offences.[15]

6.25 The AFP noted that identity crime is often linked to other forms of criminality, including illicit commodity movements, money laundering, fraud against the Commonwealth, people smuggling and human trafficking.[16] Additionally, the AFP submitted that the organised theft and sale of stolen identity information was usually for the purposes of manufacturing fraudulent identity documents, including credit

---

11 Mr Paul Dickson, Assistant Commissioner, South Australian Police, *Committee Hansard*, 9 September 2014, p. 10.

12 Mr Paul Dickson, Assistant Commissioner, South Australian Police, *Committee Hansard*, 9 September 2014, p. 10.

13 Mr Stephen Fontana, Assistant Commissioner, Victoria Police, *Committee Hansard*, 9 September 2014, p. 57.

14 *Journals of the Senate*, No. 79—2 March 2015, p. 2203. Information about the Senate Economics References Committee inquiry into digital currency can be found here: www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency.

15 AFP, *Submission 6*, p. 1.

16 AFP, *Submission 6*, p. 5.

cards, driver licences and Medicare cards. All of these documents can be subsequently used for criminal purposes.[17]

6.26 In relation to the level of identity crime in Australia, the AFP noted:

> The extent and impact of identity crime in Australia remains difficult to establish definitively. The Australian Bureau of Statistics Personal Fraud Survey for 2010-11 estimated over 700 000 Australians were victims of identity fraud and over 44 000 Australians were the victims of identity theft.[18]

6.27 The AGD elaborated on this point noting that surveys by the Australian Institute of Criminology (AIC) and Australian Bureau of Statistics (ABS) indicate that around 4 to 5 per cent of Australians report being a victim of identity crime each year, and have suffered subsequent financial loss. The AGD quantified the financial losses experienced by victims of identity crimes:

> The AIC survey indicated that victims reported an out-of-pocket loss of between $1 and $310,000, at an average of $4,101 per incident. However, just over half of respondents (55%) who reported losing money managed to recover or be reimbursed for some of their losses, at an average of $2,481 per incident, while the remaining 45 per cent did not receive any reimbursement or recover any losses. Overall, losses were relatively small, with 50 per cent of victims losing less [than] $250 and 75 per cent losing less than $1000.[19]

National Identity Security Strategy

6.28 The National Identity Security Strategy (NISS) was developed in 2005, following a Council of Australian Governments (CoAG) agreement to recognise that preservation and protection personal identity information 'is a key concern and a right of all Australians.'[20]

6.29 In 2012, the NISS was revised to 'support the development and implementation of the identity crime measurements framework.'[21] The AFP submitted that the NISS aims to develop conditions where Australians feel confident they enjoy the benefits of a 'secure and protected identity':

> The scope of the NISS is shaped by the need to strengthen national security, prevent crime and enable the benefits of the digital economy. Commonwealth, state and territory Governments are working together to enhance national consistency, interoperability and opportunities (including for government service delivery) through nationally consistent processes for

---

17 AFP, *Submission 6*, p. 5.

18 AFP, *Submission 6*, p. 5.

19 AGD, *Submission 9*, p. 14.

20 Attorney-General's Department, *National Identity Security Strategy*, www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx, (accessed 26 June 2015).

21 AFP, *Submission 6*, p. 13.

> enrolling, securing, verifying and authenticating identities and identity credentials.[22]

6.30 The AGD submitted that the DVS was a key element of the NISS.[23]

Document Verification Service

6.31 The committee heard evidence from numerous witnesses, including the AGD, ABA and remittance industry participants regarding the DVS, which is used by financial service providers to validate the identity of customers. The feedback on the DVS was largely positive, however some witnesses, including the ABA, criticised the cost of access and the limited information available to financial service providers.

Background

6.32 The DVS is a secure, online system that 'provides for automated checks of the accuracy and validity of information on the key government documents commonly presented as evidence of identity.'[24] The AGD submitted that the DVS allows user organisations, like banks and other financial services providers, to check the information on identity credentials against the records of issuing agencies.

6.33 The DVS has been available to government agencies since 2009. Certain private sector organisations, which have requirements to verify identities under Commonwealth legislation, gained access in early 2014.[25] The AGD noted:

> There has been strong private sector interest in the DVS, particularly from providers of financial services. As at 29 April 2014, 160 private sector applications had been approved and the service had 23 active private sector users. On 5 May 2014, the Attorney-General, Senator the Hon George Brandis QC, launched the DVS commercial service.[26]

6.34 The AGD was emphatic in its view that the DVS helps businesses protect themselves against identity crime while making identity verification mandated by legislation easier. Further, the AGD submitted that the DVS was not a database in that it did not retain personal information, and that all checks must be carried out with the informed consent of the individual. Finally, the AGD noted it was working with State and Territories (as joint owners of the DVS) to further expand the range of private sector organisations that have access to the service.[27]

---

22 AFP, *Submission 6*, p. 13.

23 Attorney-General's Department, *National Identity Security Strategy*, www.ag.gov.au/rightsandprotections/identitysecurity/pages/nationalidentitysecuritystrategy.aspx, (accessed 26 June 2015).

24 AGD, *Submission 9*, p. 16.

25 AGD, *Submission 9*, p. 16.

26 AGD, *Submission 9*, p. 16.

27 AGD, *Submission 9*, p. 16.

Responses from private sector DVS users

6.35 The ABA argued that while the DVS was a step in the right direction in enabling private sector operators to access verified identity data, it suggested that government and industry should work together to create a 'secure digital identity' for Australians.[28]

6.36 Independent remittance industry representatives noted that there are costs to private sector users of the DVS, including being charged 67 cents to check identities (per successful check) and paying a $5000 set up fee.[29] The independent remittance industry association, subsequently known as the Australian Remittance and Currency Providers Association, submitted that the $5000 set up fee ought to be waived. The association argued that the removal of the fee would allow remittance providers of varying sizes access to the DVS.[30]

6.37 Similarly, representatives from Veda, a data analytics company with a background in identity security and fraud prevention, argued for easier access to the DVS. Veda representatives contended that the VDS did not include enough data and was not accessible to numerous stakeholders who require identity verification technology.[31]

6.38 Veda submitted that the DVS, while verifying the authenticity of government issued identification, is only available to organisations with a requirement under Commonwealth legislation to verify identities.[32] Veda submitted that 'the restriction on access must end,'[33] and was also critical of the fees charged for access, arguing that the high fees had resulted in low numbers of subscribers:

> Fifteen months after opening, only 200 entities have applied. Consider the real estate agent letting a property or the utility providing energy. As the South Australian police submission points out, organised criminal syndicates are involved in cannabis-growing houses with rentals under false names. We ask that the committee recommend that the DVS should be open to any entity with a reasonable requirement to verify identity and have subscriber requirements similar to those used to subscribe to other government registers, such as ASIC's Personal Property Securities Register. We also note, reflecting the varying unreadiness of state registers, that the

28 Mr Guy Boyd, Global Head of Financial Crime, Australia and New Zealand Banking Group Ltd, *Committee Hansard*, 9 September 2014, p. 3.

29 Ms Dianne Nguyen, Director, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 27.

30 Australian Remittance and Currency Providers Association, *Supplementary Submission No. 2*, p. 2.

31 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

32 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

33 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

> DVS cannot verify birth, death and marriage certificates online and in real time. This in the digital age needs remedying.[34]

6.39 Veda argued that a more widely available and cheaper DVS, together with changes to the restriction on access to electoral roll and credit reporting data would 'add integrity to the first layer of identity checking'.[35]

Response from AGD

6.40 In answers to *Questions on Notice*, the AGD detailed its proposal to the Law Crime and Community Safety Council (a council of COAG) that the DVS should be open to any organisation that has a reasonable requirement to identify a person to conduct their business and obtains that person's consent. According to the AGD, this would be consistent with the *Privacy Act 1988*, including the revisions that came into effect in March 2014.[36]

6.41 The AGD advised that it expected to implement the new access policy for all jurisdictions that have agreed to the arrangements, in March 2015.[37] The AGD has also reviewed the process to access to the DVS:

> The Department will implement a substantially simplified application process in March 2015. The per user access fee will be significantly reduced as a result.[38]

6.42 Expanded access to the DVS became effective on 31 March 2015. The DVS website notes that 'businesses with a reasonable need to use a Commonwealth identifier to verify their client's identity may now be eligible to access the DVS.'[39] The changes made to DVS access include:

- a reduction in access (or 'set up') fee from $5000 to $250;[40] and
- a change to fee structure so that fees are charged per identity check. Details of these fees are outlined in Table 1 below.

---

34 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

35 Mr Matthew Strassberg, Senior Advisor, External Relations, Veda, *Committee Hansard*, 9 September 2014, p. 36.

36 AGD, *Answers to Questions on Notice*, p. 4.

37 AGD, *Answers to Questions on Notice*, p. 4.

38 AGD, *Answers to Questions on Notice*, p. 4.

39 Attorney-General's Department, *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

40 Attorney-General's Department, *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

Table 1—DVS fees schedule, as at 10 June 2015[41]

Annual Volume	Per calendar month	Per query charge
< 400 000	<33 000	$1.40
>400 000 <600 000	>33 000 <50 000	$1.20
>600 000 <800 000	>50 000 <65 000	$1.00
>800 000 <1 million	>65 000 <85 000	$0.80
> 1 million	>85 000	$0.65

Committee view

6.43 The committee acknowledges the ongoing threat of identity crimes.

6.44 The committee welcomes the major reduction in the DVS registration fees and is satisfied with the efforts of the AGD to broaden access to the system. The committee is confident that over time this will lead to many more private sector organisations accessing the DVS facility, and in turn improve personal identity security in Australia. In the committee's view the DVS will become a keystone for government agencies and private companies who require verification of a client's identity.

Support for victims of identity crime

6.45 In 2014, the Minister for Justice launched iDcare, a national support centre for victims of identity crimes.[42] iDcare argued that since 2003, financial crime in Australia has evolved rapidly and mirrors developments in commerce, government services and mobile communications.[43]

6.46 iDcare argued that the previous ten years has also seen the advent of technology-based identity crime, where motives have expanded from traditional financial gain and theft of personal or financial information, to political or ideological statements, known as *Hacktevism*. iDcare submitted that it viewed *Hacktevism* crimes as more personalised than 'traditional' identity theft, and that it had responded to over 800 individual clients since September 2013, some of whom had been victimised by *Hacktevism*, 'the consequences of which can have quite different impacts to individuals.'[44]

41 *The Document Verification Service—fast, secure, trusted*, www.dvs.gov.au/Pages/default.aspx (accessed 10 June 2015).

42 iDcare, *Submission 23*, p. 1.

43 iDcare, *Submission 23*, p. 1.

44 iDcare, *Submission 23*, p. 2.

6.47 Critically, iDcare estimated that 1.1 million Australians and New Zealanders are impacted by identity theft and misuse of information every twelve months.[45]

6.48 iDcare raised specific issues relating to Commonwealth victim certificates, which are designed to support claims for victims of Commonwealth identity crime. iDcare noted that under the current scheme individuals must satisfy three criteria:

- a person makes, supplies or uses identification information (yours, or a third party's);
- they do this intending that either they or someone else will pretend to be you or another person (who is living, dead, real or fictitious); and
- the act of pretending would be done to commit or help commit a Commonwealth indictable offence.[46]

6.49 iDcare argued that these criteria were difficult to fulfil given that less than six per cent of identity crime perpetrators are arrested or prosecuted successfully.[47] iDcare contended that the certifications are not working to support victims of identity crime:

> iDcare is not aware of any successful issuance of a victim certificate for identity crime, within either relevant State equivalent measures or the Commonwealth. This is not from a lack of interest. iDcare receives a number of calls from individuals that express interest in obtaining such certificates, but in all instances fall at the first hurdle of the essential element – someone has been successfully convicted of an identity crime offence.[48]

Committee view

6.50 The committee is concerned with the evidence from iDcare about the prevalence of identity crime in Australia.

6.51 The committee is also greatly concerned with the evidence that Commonwealth victim certificates appear to be difficult to obtain due to evidence that an arrest and successful prosecution being required to satisfy the first eligibility criterion. Given the seriousness of the problem, the significant personal impacts suffered by the victims of identity theft, and the likelihood of increasing incidences of identity crime, the committee believes there is further work to be done to both deter identity crime and to assist its victims.

6.52 The committee commends iDcare for its work in assisting the victims of identity crime, and is persuaded by its advocacy that the scheme for issuing Commonwealth victim certificates needs to be examined.

---

45 iDcare, *Submission 23*, p. 1.

46 iDcare, *Submission 23*, p. 4.

47 iDcare, *Submission 23*, p. 4.

48 iDcare, *Submission 23*, p. 4.

Recommendation 11

6.53 The committee recommends the Attorney-General's Department review the arrangements for victims of identity crime to obtain a Commonwealth victim certificate.

Contactless payment technology

6.54 As outlined above, the DVS is an effective tool for both law enforcement and financial service providers for checking and verifying the identities of customers accessing financial services. Critically, the related issue of technology-enabled credit card fraud was raised by numerous submitters, including law enforcement agencies, who argued that new technology had effectively expanded the scope for credit card fraud from more traditional credit card fraud, to multiple low value purchases to evade detection. This, they argued, was largely due to the rollout of contactless payment technology.[49] This section addresses some of that commentary in detail.

6.55 Contactless payment technology enables customers to pay for products and services under $100, by 'waving' or 'tapping' their card to payment terminals. Benefits for customers include faster transactions and in some cases, the ability to pay through the use of 'near field communication' technology in mobile phones.[50]

6.56 Victoria Police raised as an area of concern a 'significant increase' in deception offences in Victoria, arguing that new technology had enabled offenders to commit multiple low value transactions with stolen credit cards.'[51]

6.57 Victoria Police argued that increased technology, lack of guardianship and the perception that credit card fraud is a victimless crime, is 'driving [deception] offences'.[52] Victoria Police also argued that 'tap and go' technology, provides motivation for the physical theft of credit cards, with little risk of capture by police or of physical identification. Further, Victoria Police noted:

> The major banks provide a Zero Liability Policy to customers who are victims of fraudulent transactions. This policy is clearly advertised in conjunction with ‘Tap and Go’ technology. Widespread promotion of the Zero Liability Policy is expected to motivate offenders who are likely to see that the victim will not be at a personal loss. Anecdotal information from the Victoria Police Fraud & Extortion Squad and Victoria Police E-Crime Squad suggests that financial institutions factor fraudulent activity into their profit and loss margins and currently the loss associated with ‘Tap and Go’

---

49 Contactless payment refers to technology that allows individuals to pay for products and services by 'tapping' their credit or debit card against a payment terminal. The committee recognises numerous iterations of this technology exist and are referred to, in some cases interchangeably as 'tap and go', 'paywave' and 'paypass'.

50 Visa, Mobile Visa payWave, http://www.visa.com.au/personal/features/include/Visa_mobile_payWave_factsheet_approvedApril2014.pdf (accessed 30 June 2016)

51 Victoria Police, *Submission 13*, p. 2.

52 Victoria Police, *Submission 13*, p. 2.

> is far [outweighed] by the profits generated. If losses are budgeted for, Victoria Police are likely to find it difficult to develop strategies in partnership with financial institutions to improve guardianship. As part of a recent intelligence gathering exercise, National Australia Bank, Commonwealth Bank, ANZ, Westpac and Visa were all contacted via email and/or phone for consultation during recent analysis of this issue by Victoria Police. No responses were received prior to the finalisation of a recent intelligence product. Without engagement by financial institutions it is difficult to understand the full extent of fraudulent activity and the impact new technology and policies have on the criminal environment.[53]

6.58 Broadly, Victoria Police were highly critical of the lack consultation between financial institutions and the police, especially as it relates to the introduction of new, higher risk technologies, such as contactless payment systems:

> Engagement with police prior to such initiatives would greatly assist in having standard practises across industry. Simplicity of structures and processes is essential and "bureaucracy" is often a barrier to effective joint action.[54]

6.59 The committee is aware of the commentary regarding the roll out of contactless payment technology, including media articles detailing police concerns about the security of the systems. Victoria Police have also raised this issue publicly, arguing that it was likely to be behind the rise in 100 extra credit card deceptions per week.[55]

6.60 Representatives of the banking industry disagreed that contactless payment technology poses a significant fraud threat. Mr Boyd argued:

> But the PayWave mechanism itself is not a large driver of fraud losses for consumers or the banks. It is actually very popular with consumers too, because it is very convenient, and it is popular with merchants because it is fast. And at the moment with the low thresholds on that mechanism I do not think it is a realistic large threat to fraud losses. I think some of the other issues we have been discussing are much bigger threats in terms of financial loss and customer inconvenience.[56]

Committee view

6.61 The committee shares the concerns of law enforcement agencies that the rollout of new technology without consultation with law enforcement agencies has the potential to become a driver of financial related crime. The committee believes that banks and other financial service providers ought to consider law enforcement issues

---

53 Victoria Police, *Submission 13*, pp 2–3.

54 Victoria Police, *Submission 13*, p. 5.

55 9news, *Credit card crime increase could see tap-and-go gone*, www.9news.com.au/technology/2015/01/17/07/50/credit-card-crime-increase-could-see-tap-and-go-gone, (accessed 20 April 2015).

56 Mr Guy Boyd, Global Head of Financial Crime, Australian and New Zealand Banking Group Ltd, *Committee Hansard*, 9 September 2014, p. 7.

more carefully, and to facilitate discussions with law enforcement about new technologies prior to rollout.

6.62 As discussed in Chapter 5, the committee is persuaded of the advantages of close private and public sector collaboration in addressing financial related crime.

6.63 While banks have argued the fraud risk of new technologies is accounted for in their banking systems, the committee believes that consumers should have the option of disabling contactless payment features.

Recommendation 12

6.64 The committee recommends that financial institutions which issue debit and credit cards create an 'opt in' function that requires customers to consent to contactless payment technology features being activated on their cards.