Chapter 4

Issues affecting the financial services, remittance and self-managed superannuation sectors

4.1 The committee received evidence relating to the licensing and registration issues facing actors within the financial services sector. While many witnesses agreed that law enforcement agencies were working effectively in deterring financial related crime, some in the finance sector criticised aspects of the law enforcement framework, arguing that significant changes are required.

4.2 This chapter examines regulatory issues from the perspective of financial services providers, and focuses on several areas, including:

- the regulatory environment monitored by ASIC and the questions of disproportionate penalties for registered and unregistered entities;
- questions about ASIC's willingness to take regulatory action against 'live scams';
- registration under the AML/CTF regime, and criticism of AUSTRAC's positioning within the sector as a law enforcement agency;
- criticism of perceived unwillingness of AUSTRAC to take regulatory action and the significant remittance industry 'de-banking' issue;
- risks arising from the IVTS; and
- risks to the self-managed superannuation sector.

4.3 An ongoing theme of the evidence was the perception that the financial services sector registration and licencing regime policed by ASIC was inadequate and unfair, and that ASIC ignored the greater risks posed by unregistered and unlicensed operators. While AUSTRAC's role as regulators has been discussed in Chapter 3, this chapter will examine instances where ASIC and AUSTRAC have used, or attempted to use, their regulatory powers to prevent financial related crime.

Registration by ASIC

4.4 There are two significant issues that were raised with reference to ASIC and its management of its regulatory responsibilities. The first relates to the penalties applied to non-compliance by licensed operators compared with penalties imposed against unlicensed operations. The second relates to ASIC's ability to use its regulatory powers to intervene in ongoing scams in a digital environment, especially when peak bodies and banks have directly contacted ASIC requesting its intervention. These two issues are addressed below.

4.5 Some submitters were critical of aspects of the financial services sector regulations, as well as the role of ASIC itself. The National Credit Providers

Association[1] (NCPA), for example, questioned a regulatory regime wherein licensed operators are penalised more than illegal unlicensed operators.

4.6 ASIC submitted that, as the financial services regulator, it has a responsibility to administer the Australian Financial Services (AFS) licensing regime and 'monitor financial services business to ensure that they operate efficiently, honestly and fairly.'[2]

4.7 ASIC noted its role as a primary law enforcement agency in the fight against financial crime, through its regulation of Australian companies, financial markets, financial services organisations and professionals. ASIC submitted that combatting financial crime was a key part of its role as a regulator:

> Given that financial markets and large pools of savings will attract those with criminal intent, combatting financial crime is a key part of our remit. Where we detect serious misconduct that is intentional, dishonest or highly reckless, we may take criminal enforcement action.[3]

Australian Financial Services Licenses

4.8 ASIC is responsible, under the ASIC Act, for the regulation and licensing of businesses engaged in consumer credit activities, including banks, credit unions, finance companies, and mortgage and finance brokers.[4]

4.9 ASIC is also the corporate regulator which is responsible for ensuring that companies, schemes and related entities meet their obligations under the *Corporations Act 2001*. ASIC registers and regulates corporations at every point, from their incorporation through to their winding up. ASIC is also responsible for ensuring that company directors comply with their responsibilities under the ASIC Act:

> Directors, company officers, auditors, liquidators and market participants play a key role in ensuring that Australia's financial markets are fair and efficient. We take enforcement action against these gatekeepers to promote fair and efficient financial markets.[5]

Penalty regime

4.10 Some submitters, including the NCPA, argued that registered operators who inadvertently breached the AFS regulations (regulated by ASIC) through incorrect legal advice or interpretation would be penalised significantly more than an unlicensed operator. The NCPA suggested that this effectively creates incentives to act as unlicensed operators:

---

1 Please note, the NCPA was previously known as the National Financial Services Federation. Its original name is used for its submission and in the *Hansard* transcripts. The committee attributes this evidence to the NCPA throughout this report.

2 ASIC, *Submission 21*, p. 3.

3 ASIC, *Submission 21*, p. 2.

4 ASIC, *Submission 21*, p. 3.

5 ASIC, *Submission 21*, p. 5.

> The penalty for unlicensed activity, if someone is caught…is one penalty unit for unlicensed activity. The legislation says that you will be fined this amount of money. However, a licensed lender who is doing the right thing and who may unintentionally get it wrong through incorrect legal advice or incorrect interpretation can be fined many times that single penalty unit, even though they are licensed and attempting to do the right thing. We say that the penalty for unlicensed activity needs to be many times that of what an entity trying to do the right thing can be fined.[6]

4.11 The NCPA was also critical of the original policy development of the *National Consumer Credit Protection Act 2009* (NCCP Act), arguing that it was underpinned by incorrect assumptions that would cause significant ongoing issues and result in penalties that cannot adequately discourage unlicensed activities:

> The original Treasury policy development for the NCCP Act 2009 incorrectly assumed that all lenders would apply for and obtain a licence and hence comply with the new Act. As a result, the penalties for unlicensed activity are manifestly inadequate to discourage unlicensed activities.
>
> It appears that the 'prime directive' for the regulator (ASIC) is to focus on the licensed lenders (who are continually bending over backwards to comply with the law) and not the illegal unlicensed entities which were in, or have entered, the market.[7]

4.12 Further, the NCPA argued that because the core objective of the NCCP Act was to ensure ASIC's focus remained on monitoring and reviewing licensed activities, penalties in the Act also focus on breaches of licensed activities as opposed to unlicensed activities.[8] The NCPA insisted that the current regulatory regime was too onerous for licensed lenders, and that businesses attempting to follow regulations could be shut down for minor non-compliance issues:

> Civil and Criminal penalties are now so onerous for licensed lenders complying with the Act for responsible provision of consumer credit that Australian Credit License holders dare not operate outside the Act.
>
> Further-more, after spending ten's, sometimes hundreds of thousands of dollars to gain an Australian Credit License, lenders may have their business shut down for non-compliance. The "incentive" for licensed lender to do the right thing cannot be overstated.[9]

4.13 Finally, the NCPA noted that the maximum penalties for licensed lenders for non-compliance was a $340 000 penalty, in addition to a criminal penalty of up to 200

---

6 Mr Philip Johns, Chief Executive Officer, National Financial Services Federation, *Committee Hansard*, 9 September 2014, p. 22.

7 National Financial Services Federation, *Submission 3*, p. 6.

8 National Financial Services Federation, *Submission 3*, p. 6.

9 National Financial Services Federation, *Submission 3*, p. 6.

penalty units ($34 000) with up to 2 years imprisonment. Conversely, the same maximum penalty applies to unlicensed activities.[10] The NCPA argued:

> In all cases penalties for unlicensed activity should be many times that of those who go to the trouble of applying for a licence and becoming licensed, but who may fall foul of the law.[11]

Committee view

4.14 The committee is concerned that the evidence presented by the NCPA demonstrates disparities within the current financial services licensing and registration system regulated by ASIC. This imbalance is highlighted by the example of the maximum penalty for non-compliance by licensed operators being equal to the maximum penalty for providing unlicensed services. The committee agrees that this has the potential to incentivise unlicensed activities, which in the committee's view should be discouraged as such activities can be used to perpetrate financial scams.

4.15 In this regard the committee notes a recent recommendation of the Senate Economics References Committee 'that the government commission an inquiry into the current criminal and civil penalties available across the legislation ASIC administers.'[12]

Recommendation 6

4.16 The committee recommends that the government review the penalties prescribed under financial services legislation administered by ASIC, with a view to achieving a better balance between non-compliance by licensed operators and unlicensed operations.

ASIC's response to 'live' scams

4.17 The NCPA was especially critical of ASIC's reaction to reports of a scam that misused a member's AFS Licence information. The NCPA extensively detailed the scam that was reported to ASIC for investigation:

> On the day I [Mr Philip Johns, Chief Executive Officer, National Financial Services Federation] found out about it, we…informed by email the ASIC credit team in Sydney. Our organisation lodged on behalf of our member. We called ASIC and reported it via their complaint line. We also send the details of the scam to the ASIC email address: feedback@ASIC.gov.au. We informed our members of the mechanics of the scam. That was on day zero as far as we were concerned. Three days later, the second member reported the same scam. Again, details were sent to ASIC regarding that. On day 3, because the information we had was live data—it had the actual Commonwealth Bank BSB, the account number, the account name and what appeared to be local phone numbers, I passed the information on to

10 National Financial Services Federation, *Submission 3*, p. 6.

11 National Financial Services Federation, *Submission 3*, p. 7.

12 Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, June 2014, Recommendation 41, p. xxxi.

> the Australian Bankers' Association, who assigned a person to assist with this. The ABA contacted the Commonwealth Bank to give them notice that these couple of accounts were being used in the scam. I am not sure of the time line the Commonwealth Bank shut that down. On day 6…ASIC rang one of our members and sent an email with receipt of what they called 'concerns received'. From our point of view, it was not concerns; this was hard, cold factual information, including the BSB and account number, of where consumers were depositing money with regard to this scam. That email on day 6 was to set up a teleconference further down the track for the investigators to talk to the members and me.
>
> On day 18, I got an email from the ABA saying he had been advised by ASIC that they had been aware of this type of scam since July. So it had run from July to November before one of our members had picked it up, but ASIC had been aware of it since July. We showed our members the tools on how to scan the internet to see whether their logos, names, licence numbers were being used by other entities on the net. Then a third member picked up their live Australian credit licence number and details being used in a scam. That was also sent to ASIC. On day 101 after we made contact with ASIC, ASIC issued media release 14-040, but, based on the information we got from the ABA, this public warning notice—and it was titled 'ASIC warns Australian borrowers about overseas lending scam'—was 223 days after ASIC supposedly became aware of the issue, which goes to the crux of what we tried to highlight in [our submission].
>
> I had a fairly frank conversation with one of the investigators, who said that basically ASIC (1) does not have the technology to try and track down these scams, (2) does not have the resources to do this and (3) the processes of natural justice, of deciding whether this even falls within ASIC's gamut to investigate then allowing all this, appear to be based…on paper, fax and letter-type dealing with the process rather than the fact that we are in a global economy and these scams are over and done with very rapidly. And they can scam thousands of details very quickly once they are up and running. So that is the time line, and this is why it is a concern.[13]

4.18 The committee subsequently provided this example to ASIC for comment, noting the significant delay in regulatory action when detailed information of the scam had been provided so promptly. In answers to *Questions on Notice* ASIC explained:

> ...in line with our approach to disrupt scams and protect consumers, ASIC determined that the most appropriate regulatory response in the circumstances was to issue a media release to educate members of the public and to disrupt the scam. Following this, ASIC published 14-040MR *ASIC warns Australian borrowers about overseas lending scam* on 10 March 2014 which was in fact about 137 days after ASIC first became aware of the issue.[14]

13 Mr Philip Johns, Chief Executive Officer, National Financial Services Federation, *Committee Hansard*, 9 September 2014, pp 23–24.

14 ASIC, *Answers to Questions on Notice*, p. 4.

Committee view

4.19 The committee is concerned about ASIC's response to the scam against NCPA's members for three reasons. Firstly, whether it took ASIC 223 days or 137 days to respond to the active scam detailed above, the committee considers ASIC's response was extremely tardy. The committee acknowledges that this incident may be an aberration, and may not be representative of ASIC's usual response timeframe. However, on the evidence before the committee, this does not appear to be the case, as ASIC was invited to respond directly to the issue and its response did not contend that this was an isolated incident.

4.20 Even if it is assumed that ASIC's typical handling time is twice as fast as its reaction in this example, the implication is that ASIC's response, from the day it becomes aware of these sorts of financial related crimes, is between 65–110 days. At best this is equivalent to more than 2 months, at worst nearly 4 months.

4.21 As many witnesses have observed, the use of modern technologies makes the transacting of internet scams incredibly rapid. If ASIC is to deal with internet-based financial related crimes in an effective manner into the future, it must improve its response times to preventing and disrupting such criminal activities.

Recommendation 7

4.22 The committee recommends that ASIC consider and then implement mechanisms to make its response to internet-based financial related crimes far more expeditious.

4.23 In this regard the committee notes several recent recommendations of the Senate Economics References Committee in relation to ASIC's complaints handling process.[15]

4.24 The committee also notes the government's response, which states that ASIC 'will undertake a formal review of its complaints management processes in 2016 to ensure that the improvements it has made have led to a more effective handling of alleged misconduct reports.'[16] As part of this formal review, the committee expects ASIC to examine whether a scam, such as the one raised by the NCPA, would be dealt with more effectively and expeditiously through ASIC's improved complaint handling processes.

4.25 The committee's second concern raised by the NCPA evidence is that ASIC's primary action, when presented with details of an active scam, was to issue a press release. In the committee's view ASIC's response by media release does not send a sufficiently robust deterrence message to future internet scammers.

4.26 Mr Johns' account of his discussion with an ASIC investigator raises questions for the committee about ASIC's technological capacity to detect and monitor

---

15 Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, June 2014, Recommendations 18–20, pp xxvi–xxvii.

16 Government response, Senate Economics References Committee, *The performance of the Australian Securities and Investments Commission*, (October 2014).

financial related crimes. Critically, the government and the Parliament must be assured that ASIC has the technological capacity to effectively and appropriately deploy its regulatory powers. For this reason the committee recommends an audit of ASIC's technological capabilities.

Recommendation 8

4.27 The committee recommends that the Australian National Audit Office conduct a performance audit of ASIC's technological capacity, and provide a report to the Parliament outlining ASIC's technological requirements and capabilities, and the extent to which any deficiencies may hamper ASIC's regulatory responsibilities.

4.28 The committee is of the view that ASIC needs to build stronger partnerships with the private sector to more effectively interact with relevant organisations to detect and deter financial related crimes. The NCPA's example shows how the intervention by the Australian Bankers' Association prompted action by the Commonwealth Bank to close down the sham accounts. In the committee's view, ASIC should have taken similar action as soon as it became aware of the internet scam.

Recommendation 9

4.29 The committee recommends that ASIC strive to improve its relationships with the private sector in order to better detect and deter financial related crimes.

Registration by AUSTRAC

4.30 Similar to the criticisms detailed above of ASIC, AUSTRAC was also criticised for not taking strong enough compliance action against operators who were not discharging their obligations under the AML/CTF regime, or complying with AUSTRAC's instructions.

4.31 One concern raised by independent remitters was that penalties were poorly targeted, and that licensed operators were often punished more severely than unlicensed operators, who faced little or no financial penalty.

4.32 AUSTRAC's submission discussed the detection of Australian-based remittance services that had been used to launder money. While AUSTRAC did not disclose the proportion of businesses that are engaged in money laundering, it did suggest that:

> ...law enforcement agencies have detected cases where Australia-based remittance businesses are used as a third party to move funds or settle transactions involving two or more foreign countries. Similar to cuckoo smurfing, this involves overseas-based remittance dealers accepting legitimate transfer instructions from innocent parties (for example, to import or export goods) but instead of conducting the transfer themselves they send instructions to Australian counterparts. This is common practice among alternative remittance businesses, as part of their routine settlement of debts, to ease cash flow constraints or take advantage of foreign exchange differences.

> However, some Australian remittance dealers have exploited this opportunity to launder cash from Australian organised crime by transferring it to recipients overseas. Likewise, the overseas remittance dealers supply 'clean' cash to overseas-based crime groups with links in Australia.[17]

4.33 AUSTRAC noted that it was able to impose civil penalties against reporting agencies when they failed to take reasonable steps to comply with their obligations as set out in the AML/CTF Act and associated regulations:

> AUSTRAC has increased its enforcement action since the commencement of the AML/CTF Act in 2006. Most of the obligations under the AML/CTF Act did not come into effect until two years after its commencement, at which time reporting entities were subject to a two-year Policy (Civil Penalty Orders) Principles period. This meant that AUSTRAC could initiate civil penalties against reporting entities only when the entities had failed to take reasonable steps to comply with their obligations. AUSTRAC was well placed, as a result of strengthening its enforcement capability, to take action when non-compliance was identified and the full suite of powers came into effect from 2008.[18]

4.34 To minimise the high risks associated with the remittance sector in general, AUSTRAC noted that changes were enacted to the AML/CTF Act in 2011 to both strengthen the registration requirements for remitters, and to enhance the AUSTRAC CEO's powers to deal with compliance issues.[19]

4.35 While representatives of the independent remittance sector acknowledged that the sector is deemed high risk, they noted that since 2012, many previously unregistered operations had subsequently registered with AUSTRAC.[20]

4.36 AUSTRAC has to date used these new powers (to refuse, suspend or cancel registration) only once. However, it noted that it had placed conditions on the registration of numerous agencies (15 instances as at May 2014), as well as imposing significant financial penalties on remittance network providers for failing to register affiliates and providing services through unregistered affiliates.[21]

4.37 Independent remitters suggested that current regulatory arrangements were not sufficient to deter unregistered remittance operators. Further, they argued that it may be easier for an unregistered remitter to operate than previously:

---

17 AUSTRAC, *Submission 10*, p. 13.

18 AUSTRAC, *Submission 10*, p. 27.

19 AUSTRAC, *Submission 10*, p. 13.

20 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 28.

21 AUSTRAC, *Submission 10*, p. 13.

> We have a subset of unregistered remitters now. If the registered remitters …close up shop, and a new flurry of unregistered remitters will come to fill the space that the registered remitters [occupied]…[22]

4.38 AUSTRAC's detractors noted that there was evidence to suggest that unregistered remitters could, and were still, operating effectively without the real threat of regulatory action by AUSTRAC.[23]

4.39 AUSTRAC countered that there was a degree of regulatory engagement with unregistered remitters, citing *Taskforce Eligo (Eligo)* (as discussed in Chapter 3) as an example. AUSTRAC argued that together with other law enforcement agency partners, it is detecting and engaging with unregistered remitters:

> With unregistered remitters, it would not be true to say there is no regulatory engagement with them. You will have heard detailed information, I think, from some of the earlier witnesses about Taskforce Eligo, for example, where we are working with the Australian Crime Commission and others. AUSTRAC, as part of that work, has identified people who have been unregistered.[24]

4.40 In response to criticism of AUSTRAC's engagement of unregistered remitters, AUSTRAC's former CEO, Mr John Schmidt, noted that as at September 2014, there had been prosecutions for some entities that were engaged in criminal behaviour, but that these were in concert with the ACC as part of *Eligo*:

> We do not prosecute. We are the law enforcement agency. So, to the extent that there is a breach of the criminal law, which is a criminal offence, that would be a matter for law enforcement. [25]

4.41 Critically however, Mr Schmidt did note that he was not aware of any prosecutions for 'being unregistered in itself', and noted that unregistered remitters who had been identified had been prosecuted for other (possibly related) criminal activities:

> I am not aware of a prosecution for being unregistered in itself. Having said that, unregistered remitters who have been identified as being engaged in criminal activity have been prosecuted by law enforcement for some of their criminal activities. Now, I cannot tell you, based on that analysis, who would have been potentially liable for prosecution for being unregistered.[26]

---

22 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 34.

23 Ms Dianne Nguyen, Head of Compliance, Eastern & Allied Pty Ltd, *Committee Hansard*, 9 September 2014, p. 31.

24 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

25 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

26 Mr John SCHMIDT, Chief Executive Officer, Australian Transaction Reports and Analysis Centre (AUSTRAC), *Committee Hansard*, 9 September 2014, p. 48.

Committee view

4.42 The points of contention between the disproportionality of regulatory actions against registered and unregistered remitters also feeds into the broader challenges faced by the independent remittance industry. While apparently not on the same scale as the financial services industry (and the aforementioned licensing and penalties issue), the committee agrees that the discrepancies in evidence from remitters and regulators warrants further investigation.

4.43 The committee notes that pressures on the remittance industry, including the 'de-banking' issue (discussed below) could result in a higher use or dependence on unregistered remitters.

4.44 The committee is concerned that, like ASIC, AUSTRAC is not as expeditious in moving against unregistered remitters as it ought to be. The committee believes that AUSTRAC should take a more proactive role in detecting and engaging unregistered remitters.

Recommendation 10

4.45 The committee recommends that AUSTRAC consider and then implement mechanisms to increase its regulatory oversight of the activities of unregistered remitters.

Remittance industry 'de-banking'

4.46 The committee heard from both independent and commercial remittance service providers about ongoing regulatory issues in the sector. Specifically, independent remitters argued that they were being disadvantaged by major commercial banks for two primary reasons.

4.47 Firstly, it was alleged that the major Australian banks were using changes to international anti-money laundering and counter terrorism financing arrangements to justify the closure of remitters' Australian operating bank accounts.

4.48 Secondly, it was claimed that the same major Australian banks were doing so while still offering their own remittance services, for possibly anti-competitive reasons.

4.49 The committee took these allegations extremely seriously, and heard from both the independent remittance sector and major Australian banks and the Australian Bankers Association (ABA) about this significant issue.

Account closures

4.50 Over the course of the inquiry the committee heard from numerous witnesses that the closure of remitters' bank accounts by major Australian banks was having a detrimental effect on the independent remittance industry. These concerns were first raised by representatives of the remitters' industry association, the Australian Remittance and Currency Providers Association, who argued that independent remittance services were being disadvantaged by the closure of their operating bank accounts.

4.51 Mr Crispin Yuen, Head of Compliance at Ria Financial Services Australia Pty Ltd, outlined the impact of the 'de-banking' of remittance businesses:

> Most of the major banks have decided to not bank remittance business, resulting in remittance business not having bank accounts with which to operate. This is now a pressing issue, because a business without a bank account cannot operate, and three of the four major banks have already said no. The Australian Federal Police and the Australian Crime Commission have real issues about the impact of these transactions going underground and being done by private arrangement in an unregulated, unreported way if the sector loses its banking relationships.[27]

Banks' response

4.52 The affected remitters argued that as they were complying with AUSTRAC's regulations they should not be 'de-banked'.[28] The committee invited Australia's four largest commercial banks to respond to the issues raised by the independent remittance sector.

4.53 In correspondence to the committee, Westpac indicated that domestic and international banks are finding it increasingly difficult to provide banking and payment services to remittance operators due to the Australian and international regulatory landscape and the compliance requirements in the banking industry.[29]

4.54 Westpac directed the committee to an ABA blog that summarised some of the key challenges, including that the anti-money laundering scheme in Australia which requires banks to 'know your customers'.[30]

4.55 The ABA blog outlines the domestic and international constraints the ACL/CTF requirements place on Australian banks:

> Australian banks often use overseas banks (usually in the US, UK, and EU as these are the preferred currencies) to facilitate these transactions and the law requires all banks in the value chain to meet regulatory obligations, including risk management to prevent money laundering/terrorism financing and adhere to sanctions across multiple jurisdictions. The expectation of overseas regulators and clearing banks is that international transfers represent transparency, knowing your customer, your customer's customer and who the beneficiaries are. This is not always possible and Australian banks need to take great steps not to breach both foreign and domestic law, including laws on anti-money laundering, counter terrorism financing and sanctions.

---

27 Mr Crispin Yuen, Head of Compliance, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, p. 28.

28 Mr Crispin Yuen, *Committee Hansard*, 9 September 2014, pp 28–29.

29 Westpac, *Correspondence*, p. 1, (2 February 2015).

30 ABA, *The risks of remittances*, www.bankers.asn.au/Media/ABA-Blog/Blogs/The-risks-of-remittances (accessed 29 April 2015).

> Failure to do so could result in any Australian bank that, even unknowingly, violated these laws to be instantly cut off from access to the US, UK or EU financial system, including significant regulatory action and fines which would have a devastating impact on the Australian banks and economy.
>
> Therefore, banks in Australia are assessing the risks of using remittance operators and companies, and in some cases choosing to cease providing services to ensure they do not breach international laws.[31]

4.56 In light of the requirements of financial institutions internationally, Westpac had decided 'that like most Australian banks we are not generally in a position to provide banking services to remittance businesses.'[32]

4.57 Westpac acknowledged that the account closures would affect the independent remittance industry, as well as the businesses and remittance providers that use their services.[33]

Class action by remitters

4.58 Westpac's correspondence also detailed a class action brought against it in November 2014 by a group of remitters. The action was initiated by the remitters in order to reinstate their accounts until alternative finance facilities could be found:

> The class action sought to require Westpac to provide more time to enable remitters to seek alternative banking services. In December [2014], Westpac reached an in principle agreement to settle the class action and this was approved by the Federal Court on 5 January 2015.[34]

4.59 Westpac explained that part of the settlement included keeping banking facilities open until 31 March 2015, 'to allow those customers time to make alternative banking arrangements before...services cease after that date.'[35]

Attorney-General's Department's working group

4.60 Westpac advised the committee that the government has established a working group chaired by AGD and including associated parties (regulators, banks and remittance industry associations) 'to see what longer-term solutions may be possible to support and help make such [remittance] payments in the future.'[36]

4.61 As at 23 June 2015, there is no information available on the progress of the working group, other than indications that its work is ongoing.

---

31 ABA, *The risks of remittance*s, www.bankers.asn.au/Media/ABA-Blog/Blogs/The-risks-of-remittances (accessed 29 April 2015).

32 Westpac, *Correspondence*, p. 1 (2 February 2015)

33 Westpac, *Correspondence*, p. 1, (2 February 2015).

34 Westpac, *Correspondence*, p. 1, (2 February 2015).

35 Westpac, *Correspondence*, p. 1, (2 February 2015).

36 Westpac, *Correspondence*, p. 1, (2 February 2015).

Advice from the ACCC

4.62 The committee subsequently wrote to the ACCC requesting an examination of the substantive question of whether the banks' closure of remitters' accounts amounted to anti-competitive behaviour or a misuse of market power. The ACCC was provided with copies of the committee's Hansard and related correspondence.

4.63 The ACCC's Chairman, Mr Rod Sims, responded:

> I understand that during the course of the inquiry, money remitters have raised a concern that most of the major Australian banks have stopped providing banking services to independent remittance businesses and closed their accounts.[37]
>
> You have asked whether this action may constitute anti-competitive behaviour; given the banks offer their own remittance services.
>
> Like any businesses, banks have the right to choose who they deal with and there are many reasons why a bank may legitimately refuse to supply goods or services.[38]

4.64 The ACCC noted that if the banks had acted collectively to close remitters' accounts, it would raise concerns under the cartel provisions in the *Competition and Consumer Act 2010* (the CCA).[39] The ACCC concluded that:

> …on the basis of the material available, including the Hansard transcript of the Committee's hearing, the letter from Westpac and the submission to the inquiry from the Australian Bankers' Association Inc., there is [no] suggestion that the banks have acted collectively to close remitters' accounts.
>
> Rather, the available material suggests that the major Australian banks have individually decided to stop providing banking services to independent remittance businesses as a way to individually manage their compliance risk and [to] meet their obligations under Anti-Money Laundering and Counter Terrorism Financing regulations.[40]

4.65 The ACCC remarked that if a bank had closed a remitters' account to eliminate the remitter as a competitor to the bank, it could raise concerns under section 46 of the CCA.[41] However, the ACCC noted:

> On the basis of the available material, and assuming that the major Australian banks have market power, there is no suggestion that the banks have closed remitters' accounts for an anti-competitive purpose. Instead, as noted above, it appears that the banks have individually decided to stop

37 ACCC, Correspondence, p. 1. (2 April 2015)

38 ACCC, *Correspondence*, p. 1. (2 April 2015)

39 ACCC, *Correspondence*, pp 1–2. (2 April 2015)

40 ACCC, *Correspondence*, p. 2. (2 April 2015)

41 ACCC, *Correspondence*, p. 2. (2 April 2015)

> providing banking services to independent remittance businesses in order to ensure their availability to meet their regulatory obligations.[42]

4.66 Critically, the ACCC acknowledged the importance of independent remitters to members of migrant communities in Australia, many of whom use remitter services to send money to families and friends overseas. The ACCC noted that the AGD's working group had been established to work through these issues, and offered its assistance to that process.[43]

Committee comment

4.67 The questions relating to the closure of remitters accounts are complex. In the committee's view there needs to be a suitable balance between the constraints of a robust AML/CTF regime and the ability for legitimate remittance service providers to access necessary financial products. The committee acknowledges the ongoing work of the AGD working group to find a satisfactory resolution for independent remitters' services and the communities that use them.

4.68 The committee chooses not to make any recommendations on this issue due to the ongoing considerations by the working group. The committee will monitor the groups' activities going forward, and supports a solution that takes into account the need for a robust AML/CTF regime and does not result in the closure of legitimate independent remittance service providers.

Informal Value Transfer Systems

4.69 As foreshadowed in Chapter 3, the ACC noted that *Eligo* had examined the use of the ARS and IVTS, alternatively known as Hawala, Hundi, Fei ch'ien or Phoe kuan.[44]

4.70 The ACC noted that IVTS are largely used in Australia by global diaspora communities to remit funds outside of the formal financial and banking system:

> IVTS networks represent some of the oldest and most established financial systems in the world and encapsulate a number of value transfer mechanisms that predate the modern Western notion of formal banking. Some IVTS mechanisms used today have existed as far back as 5800 BC, and include Hawala (Middle East, Afghanistan, and Pakistan), Hundi (India), Fei ch'ien (China), and Phoe kuan (Thailand). These IVTS are still in operation across the globe and are often the preferred means of transferring value in many cultures.[45]

4.71 The ACC explained that *Eligo* had been established as a result of the recognition of AUSTRAC's designation of the National Threat Assessment on Money Laundering as 'high'. The ACC Board responded in December 2012 with the establishment of *Eligo*:

---

42 ACCC, *Correspondence*, p. 2. (2 April 2015)

43 ACCC, *Correspondence*, p. 2. (2 April 2015)

44 ACC, *Submission 5*, p. 11.

45 ACC, *Submission 5*, p. 11.

> ...the ACC established Eligo to take a coordinated and collective approach against high-risk remitters and IVTS operating in Australia to reduce their adverse impact on Australia and its national economic wellbeing. The Task Force operates under the ACC's [Targeting Criminal Wealth] Determination, which allowed the ACC to utilise the full breadth of its coercive intelligence collection capabilities. The AFP and AUSTRAC were principal partner agencies involved in Eligo; however, Eligo engaged with numerous domestic and international partners...[46]

4.72 The aim of *Eligo* was to disrupt remitters and IVTS operators assessed as posing a high money laundering risk, and to implement crime prevention strategies that would optimise the use of AML/CTF regulations.[47] *Eligo* resulted in the seizure of more than $580 million in drugs and assets, including in $26 million in cash.[48]

4.73 While this is a significant success, the alternative remittance sector noted that the use of IVTS was still high among certain communities and that the effect of the closure of remitters' accounts would ultimately drive more people to use unregulated services, thus putting themselves at a great financial risk.[49]

4.74 The alternative remitters acknowledged that it was possible to operate in Australia without seeking registration, by establishing banking arrangements offshore:

> **Senator O'SULLIVAN**: Pretend I wake up one day and decide that I am going to become a remitter. I am not going to seek registration in Australia under the government's regulations here. I have just decided to establish my banking arrangements somewhere offshore. Could I function efficiently?
>
> **Mr Bieytes Corro**: Yes, you can. If you do hawala or hundi, yes, you would be able to do it. In that sense, there will not be any real money transfers happening between Australia and Hong Kong. You will just have a bank account there and a bank account here. The money is actually not being transferred. Eventually, you use the banks, if you can, to do a settlement with your counterpart on the other side—but that is unregulated.[50]

Committee view

4.75 The committee is concerned that the effect of the closure of remitters' accounts could lead to a heavier reliance on IVTS systems in some communities, potentially drawing law abiding individuals and families into the sphere of organised and serious criminal groups through a lack of financial and banking safeguards.

---

46 ACC, *Submission 5*, p. 15.

47 ACC, *Submission 5*, p. 16.

48 ACC, *Submission 5*, p. 16.

49 Mr Eduardo Bieytes Corro, Managing Director, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, 9 September 2014, p. 30.

50 Mr Eduardo Bieytes Corro, Managing Director, Ria Financial Services Australia Pty Ltd, *Committee Hansard*, 9 September 2014, p. 30.

4.76 The committee recognises that many IVTS users access those services legitimately, but also acknowledges the high risks that IVTS users are exposed to, due to a lack of regulatory action by either ASIC or AUSTRAC.[51]

4.77 The committee believes that communities should be encouraged to use registered and regulated services. To this end, the committee encourages the government, through its current law enforcement arrangements, to continue to monitor the issues raised both in *Eligo* and by submitters to this inquiry in relation to IVTS.

Self-managed superannuation funds

4.78 The committee took evidence from witnesses that superannuation investments were at particular risk of financial related crime, largely because of the increased technological management of superannuation funds.

4.79 The ABA argued that self-managed superannuation funds (SMSFs) mostly sit seemingly dormant.[52] This fact provides opportunities for criminals if they can get access to the account, and a risk that any unauthorised access may be undetectable for some time. Further, the ABA discussed the increasing use of "phishing" type scams with respect to superannuation:

> That is where we are relying on our electronic detection to pick anomalous behaviour up, but it is not perfect. There are ways around it. That is one of the things that I think is a growing area, and, of course, the criminals would see this as well. They understand that people are saving money in these locations and they are sending out letters saying, 'Roll over your super into this account.' I have received several letters saying, 'This person has left employment and could you please transfer her superannuation fund to this fund.' That was for a member of my family, so I knew it was not real, but there are just phishing expeditions going on to probably all superannuation funds.[53]

4.80 The ABA noted that accountants and lawyers are not subject to current AML/CTF regulations, and referred to them as the 'weakest link' in relation to regulation of SMSFs:

> Accountants are the people who set up SMSFs and, as with any system; criminals go to the weakest link. In the AML-CTF space, the weakest link is the accountants and lawyers because they are not regulated. There is a significant amount of money going into SMSFs and, therefore, there is the potential for those investments to be exploited for that reason for money laundering rather than fraud.[54]

---

51 See Chapter 3.

52 Mr Steven York, Head of Groups Security and Business Resilience, Bank of Queensland, *Committee Hansard*, 9 September 2014, p. 2.

53 Mr Steven York, Head of Groups Security and Business Resilience, Bank of Queensland, *Committee Hansard*, 9 September 2014, p. 2.

54 Mr Paul Stacey, Policy Director, Australian Bankers' Association, *Committee Hansard*, 9 September 2014, p. 2.

4.81 AUSTRAC also raised the vulnerability of SMSFs generally, noting that a significant amount of money in Australia is invested in superannuation funds, which provides significant challenges for law enforcement agencies to monitor. AUSTRAC mentioned the effectiveness of *Task Force Galilee* led by the ACC that targeted 'boiler room scams' in which retirees were phoned and offered investment opportunities that led to significant fraud:

> Historically, one of the ways these scammers got people's names and addresses was through various share registries and other lists which were publicly available. I am not quite sure whether they are now available to the same extent that they were. They say, 'Look, we've got a fantastic investment opportunity for you.' They lure people in. They are very sophisticated. They have websites which look legitimate. Some of the more sophisticated ones would have what appeared to be genuine share trades, which made profits. So they would bait the hook. Then they would invite investors to put more and more money into these schemes or to buy particular shares, which either did not exist or were worthless. Then the money was gone. There have been a number of examples where people have lost significant amounts of funds through scams of that nature. That is a particular area of vulnerability.[55]

Committee view

4.82 The committee is concerned with the evidence that SMSFs are particularly vulnerable to financial related crime. The committee supports the important role of Commonwealth law enforcement agencies in their work monitoring and containing the risks to SMSFs from financial related crime.

4.83 The committee urges law enforcement agencies to continue to develop new and effective methods of detecting and disrupting financial frauds perpetrated against SMSFs.

55 Mr John Schmidt, Chief Executive Officer, AUSTRAC, *Committee Hansard*, 9 September 2014, p. 46.