

Draft Scam Prevention Framework — Response

David Sweeney

October 4, 2024

Provided by email to scampolicy@treasury.gov.au. All information, analysis and opinion contained herein is provided on a best efforts basis for the sole purpose of helping the government make an informed decision regarding the proposed Scam Prevention Framework and any related efforts to prevent fraud.

The proposed Scam Prevention Framework is too cumbersome and will arrive too late. All that is required to stop scams is that with transparency for customers banks are informed of frauds. Banks can then make a financial decision about acting on that information. If they do not customers can take the information regarding what the bank knew about the fraud to the bank and point out the bank has not done all it could. Most of what is needed has been in place for many years. All that has been missing is transparency for customers and victims and a little coordination.

1 How my father was scammed and how we got the money back from the banks

In 2015/2016 my father was the victim of Option Financial Markets (OptionFM), an online fraud (scam), losing around \$1,000,000.¹ All three banks from which the payments were made refused our continued request for information on the fraudulent company Option Financial Markets (OptionFM).² In 2020 I got by FOI an ASIC warning regarding OptionFM.³ I took this warning to the three banks and they returned the lost money, as they were proven to have at least been informed about the fraudulent activity. See for example our settlement with Westpac in which my father received 100% of the money lost plus interest plus \$5k for pain and suffering.⁴

2 ASIC warning emails

Since at least 2013, but perhaps for much longer, ASIC has been sending warning emails to banks regarding online frauds.⁵ It is my understanding that from 2016/2017 these emails have been sent from AUSTRAC. As can be seen from my father's case these email are an effective way of either stopping a fraud, or if the bank does not act the email puts the victim in the position to ask that the bank admit their mistake and refund or return the money. Just one

¹See journalism see [A.1](#) and see [B](#) for an example of communications from OptionFM.

²See for example of [C.1](#).

³See [E.2.2](#).

⁴See [C.2](#).

⁵See [E.2](#) for examples and [E.1](#) for ASIC FOI decisions in which these emails were obtained.

of these ASIC emails has been made available to victims who have taken it to AFCA/FOS.⁶ AFCA/FOS have seen the relevance of the emails but have tended to set settlement at 75% of the money lost rather than the 100% that my father's case shows can be achieved approaching the bank directly.

The key here is that the scam victim needs to know what the bank knew about the fraud. In such a case AFCA will work fine but a better result can most likely be currently achieved by going directly to a bank.

The need for the victim of the scam to know this information can be seen in three AFCA/FOS cases.⁷ Here the fraudulent company is OptionFM⁸, the company that defrauded my father. Because the victims did not have access to the relevant ASIC email AFCA/FOS found against them. Neither AFCA/FOS nor the banks would or could provide the email.

I have had trouble finding anyone interested in considering the importance of this information.⁹

3 Another example of a victim knowing what the bank knew and getting money back

Another example but with knowledge about money laundering at the receiving bank can be seen in this article.¹⁰ The relevant documents were KYC (Know Your Customer) documents and were shared with the victim by the police.

4 Analysis of AFCA/FOS scam cases

In rough numbers my current analysis¹¹ suggest that of 1300 determinations that mentioned 'scam': there are perhaps 815 genuine scam cases that have reached determination and been published.¹² Of these the majority (740 or 90%) are tried on available evidence and found against the victim with most victims getting no money returned and some getting up to 10% of losses returned. A minority (65 or 8%) are tried on the available evidence and are found in favour of the victim with the victim getting between 10% and 100% of losses returned. Six cases are the above involving the ASIC email cases which are tried on the normally unavailable ASIC warning and all go to the customer with a return of 75% of the loss.

Rather than working as consumer protection to remove power and information asymmetry between bank and victim the process seems to work to justify the lack of information to the victim. AFCA treats the non-presentation by a bank of evidence that they knew about a fraud as positive proof the bank did not know about the fraud. What is worse this process, in which banks tell victims most people do not get money back after a scam and then suggest victims take complaints to AFCA and then AFCA rules that the bank has no responsibility as no

⁶See F.1. How this ASIC warning E.2.1 was provided to the victim in this FOS case F.1.1 is not clear, it does not appear to have been via FOI. ASIC has been sent an enquiry but as yet has not replied. It would seem that access to these emails, decisive for victims, has not been equal. I know that in my father's case I was told by bank staff that ASIC never sent such emails.

⁷See F.2.

⁸AFCA was asked for permission to identify OptionFM for this response. Their reply was unclear in that they simply said they could not or would not identify the company.

⁹See for example reply from the Hon. Andrew Leigh D.1.

¹⁰A.2.

¹¹I could not find on AFCA's website a better way to do this than download the PDFs manually and analyse the raw text data. Historical data does not seem to be available in an accessible form and current data does not seem to be available for easy access for research.

¹²That is cases involving fraud on the customer where the payment is authorised.

information has been provided to prove the bank knew a fraud was being committed, seems to point customers away from genuine avenues for recompense such as taking the bank to court and getting such information through discovery. I am yet to read an AFCA/FOS case in which a victim was informed of the importance of this information and told they should seek legal advice. Given the low chance of a positive outcome without information as to what a bank knew about a fraud it is hard to understand how AFCA is functioning as an alternative to court for scam cases. It is even harder to understand how it will function to police the SPF without access to this information.¹³

5 Background to SPF

The following are some of the steps on the path to the current situation.

- In the 1980s and 90s credit/debit card payments and online payments were introduced. For card payments this led to unauthorised payments increasing. For online payments the fact that payments were made using the direct entry batch system, a compersial payments system, had the direct result that names were not matched and the payments were irriversible.
- The ePayments code was in part to deal with these problems. While a moderatly good solution was found for unathorised payments the treatment of mistaken payments has never been fit for purpose.¹⁴
- ASIC warning emails sent since at least 2013 and perhaps much ealier. They may originally have been faxed. These seem to have been a subset of the ASIC “Investor Alert List.”¹⁵ ¹⁶
- In 2016/2017 AUSTRAC started sending the ASIC warning emails and adding a legal note at the end. Banks appear to have taken notice.
- Recently the excitingly named “National Anti-Scam Centre: Investment Scam Fusion Cell” would seem to be a combination of the ASIC warnings with a UK website takedown facility.¹⁷

An analysis of how these and other developments have led to Australian being the takets of organised crime on a massive scale would be insightful and appears missing from the current considerations.

¹³For example see of better advice to victims see Murray, Amelia. “Victim of Fraud? Take the Bank to Court.” *The Telegraph*, 14 January 2017. <https://www.telegraph.co.uk/money/banking/savings-accounts/victim-fraud-take-bank-court/>.

¹⁴See Tyree, Alan, 2021. *Banking Law in Australia*, 10th ed., LexisNexis. In particular ‘9.13.2.3 Internet Payments,’ pp.324-5, which contains the following suggestive comment: “The ePayments Code now earls with mistaken internet payments, but the treatment is entirely unsatisfactory, depriving the customer of benefits under the common law. In the author’s opinion, it amounts to an officially sponsored unfair contract.” See also, Tyree, Alan L. “Mistaken Internet Payments,” 2003. <https://www2.austlii.edu.au/alan/mistaken-epayments.html>.

¹⁵Currently residing at “Investor Alert List - Moneysmart.Gov.Au.” <https://moneysmart.gov.au/check-and-report-scams/investor-alert-list>. Had had different names at different times.

¹⁶What led some companies to be put on this list and others not is not clear to me.

¹⁷See “National Anti-Scam Centre Releases Its First Investment Scam Fusion Cell Report.” <https://asic.gov.au/about-asic/news-centre/news-items/national-anti-scam-centre-releases-its-first-investment-scam-fusion-cell-report/>.

Many of these developments while aiming to reduce crime and help consumers have not involved transparency for customers or victims. It would be desirable for the SPF to change this. The current proposal does not appear to do so.

6 Recommendation

Set in law that if a person is a victim of a scam/fraud then all banks involved have to hand over all relevant information as to what the bank knew about the fraud to the victim to help in their investigation. If that information shows the a bank did not do all it should have then the bank refunds that money to the victim plus interest plus 30% for distress. This information to include:

- SMR and TTR and IFTI
- All Australian Financial Crimes Exchange (AFCX)¹⁸ date on the fraud/scam.
- CCTV of account set up and withdrawals
- Copies of identity documentation used to set up accounts
- Money trail for 7 days after transfer
- Scam warnings
- Red flags
- Internal bank memos regarding the scam
- VISA and MasterCard warnings regarding the scam
- KYC (Know Your Customer) documents

Such informatoin creats legal oblications on banks without need for new legislation. For instance the oblicatoion not to turn a blind eye to fraud¹⁹ and the implied warrany created by the ASIC Act that 'services will be rendered with due care and skill.'²⁰

The AFCX, the ASIC/AUSTRAC warnings and giving this information to victims would seem to do the work of the Scam Prevention Framework without creating more legislation. The key here is being clear that scams are online fraud and that when banks are informed of fraud they have a duty to act. Once the victim knows the bank knew about the fraud the victim has a legitimate action against the bank, but it will not need to go that far as presenting the information to the bank would be enough in most cases.

Australia also needs laws equivant to Wire Fraud in the USA that make it easier for police to prosecute the criminals involved in online fraud.

7 Briefing

Please contact David Sweeney [REDACTED]

¹⁸AFCX afcx.com.au

¹⁹See for example Bryan, Michael. "Cleaning up After Breaches of Fiduciary Duty - The Liability of Banks and Other Financial Institutions as Constructive Trustees," 1995, 30. See [F.3](#).

²⁰Australian Securities and Investments Commission Act, Cth § 12ED (2001). http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/asaica2001529/s12ed.html.