

# **Response to Scams Prevention Framework**

## ***Introduction***

My name is Phillip Bryant and I am a retired IT Manager/ Company Director.

My family has experienced many scam attempts of many kinds but fortunately have only been caught by a few minor ones, remedied by credit card companies. However with the growth of AI use by criminals it is alarming how sophisticated scam attempts are becoming and how easy it is to dupe the banks into making incorrect payments.

I welcome this interesting and comprehensive approach to managing scams. I have made what I believe are a number of pertinent points which if not addressed by the framework need addressing elsewhere. I have also outlined a number of scam attempts we have experienced for you to assess how effective will this framework be in stopping them.

## ***Glaring weakness***

From the brief read I had of 80+ pages I could not understand how a scammed person could get compensation. But I have read that compensation would be a shared responsibility amongst the various agencies involved. Good idea.

But the scammed person has to prosecute all of them individually to get compensation. Madness. The only beneficiaries will be the lawyers.

Surely a better model is for the bank to handle the customer interface with rapid re-reimbursement of losses, and the bank then seeks to recover losses from the other parties. Ideally with some clear rules to ease that process, such as the 'introduction agent' pays 20%.

## ***Why only small businesses?***

Whilst the full framework may not be applicable to larger businesses they also suffer from scams and should be afforded some of the framework functions.

## ***Rapid Action***

To inspire confidence in this framework, and minimise harm, it is essential rapid action is taken. In general there is a lack of trust in government bodies as being over bureaucratic and slow. People will not use the framework if it does not result in timely action. A key success factor will be the effective implementation of IT systems to support the framework; with adequate new budgets assigned.

Given how comprehensive the framework is I can't see how it can be implemented without many years delay. Hopefully a focus on the high value elements can get quicker results.

## ***OSKO – a gift to scammers***

The introduction of the OSKO instant payments system is a gift to scammers – they can move money around in an instant and make recovery very difficult. Ideally I would like to see an option to opt out of this system on a case by case basis. As a minimum the banks could introduce a delay in that money received by OSKO cannot be resent elsewhere without either some verification method or at least a days delay.

## ***No emails/SMS with links***

We received an email from RACQ saying they owed us a refund, and click on this link to provide bank details for payment. I could not believe it – what a perfect model for scammers to use. If combined with mail hacking a simple change to the url in the message creates an ideal method for scammers to harvest bank details. I would like to see a clear message that both government bodies and business emails and SMS will never provide links for entering personal details of any sort.

Under the **Prevent** obligation I hope this behaviour can be eliminated.

## ***Confirmation of payments/ changes***

A service I welcome is the alert messages I receive whenever a payment is made from my account, or details are changed. Ideally this should be a universal requirement. This could be demanded via the **Prevent** obligation.

## ***Stronger verification***

I recall a few occasions when a credit card company has rung me to verify a transaction I have just made. This behaviour could be repeated for all large transactions, and those where money is going out of Australia. A friend of mine had his mortgage increased and the money sent abroad by a scammer and at no time was he contacted by a human to verify the transaction. This was a clear breach of the banks processes and a stronger mechanism is needed to report and

## ***Scenario – intercepted email with modified payment details***

We are one of those who received an email about our property settlement with directions as to where to pay the deposit. Fortunately I always verify large payment details by phone to a number I trust, and found the bank details had been modified. Some points arising from this:

1. This is another example of where email has been hacked, either at the agency end or the email provider. Urgent action is needed to devise secure email systems. The email received was a perfect copy of the agencies emails; and was also very timely as the payment was due.
2. The message to verify payment details cannot be emphasised enough – it's a key protection.
3. I reported the fraudulent bank account to the bank but I expect nothing happened. I hope this framework results in tighter rules around establishing bank accounts, and freezing them when suspicious activity occurs; and prosecuting those associated with the account.

## ***Scenario – scam website***

This is an example of a low value scam but probably very high frequency.

The website <https://www.ella-melbourne.com/> looks like many other Australian clothing websites, with all prices in AUD. Yet it is a Hong Kong based outfit. My wife attempted to buy something from them resulting in a foreign transaction charge. It was only after a discussion with the bank we discovered that this was not an Australian company but foreign. The following then happened:

- A dispute was lodged about the credit card transaction.
- They insisted we liaise with the (in my view) criminal outfit.
- Which I did demanding a refund due to misrepresentation.
- The outfit responded that the foreign transaction charge was beyond their scope and I should take it up with the bank.

- The ordered item was never delivered (no surprise!).
- I then raised a complaint with Westpac bank (the credit card provider) who refunded the charge.
- But they said they were not responsible for policing and could not blacklist the company.

Some points arising from this:

1. It is better to make these type of purchases with a credit card since you can usually get a refund.
2. The credit card dispute process needs updating – once evident it is a scam outfit there should be no need to liaise with them.
3. Australian rules already address one of the issues with this website – clear identification of ancillary charges (in this case a foreign transaction fee).
4. But the rules could be strengthened – there should be some way/rule that clearly identifies a website is Australian and subject to Australian laws (e.g. mandatory provision of a valid contact address and company ABN). The absence of these can lead to a presumption of a foreign site – this rule should be extensively publicised. (Note many Australian sites would currently fail this rule.)
5. With the above being mindful it would be very easy for the scammer to provide a false, or someone else's, address and ABN. An easy way to verify ABN's would be essential.
6. Under the **Detect** and **Report** obligations these cases can be collated.
7. A simple way to implement the **Disrupt** these sites would be for the credit card company to blacklist them. This is not policing (charging the companies with offences and prosecuting them) just refusing to transact with them. 3 strikes and blocked?

Will the framework be sufficient to persuade credit card providers to make more robust actions to quickly identify and block payments to scam websites?