consumer action law centre

REMEDYING SCAM LOSSES: Consumer protection is failing

Background Brief - March 2022

KEY POINTS

- **Scam losses now exceed $2 billion a year.**
- **Consumers are rarely successful in getting a refund when they make complaint to the Australian Financial Complaints Authority (AFCA).**
- **Where banks do provide customers with a refund, they provide a "low ball" offer and rarely compensate an entire loss.**
- **ASIC is proposing to reduce consumer protection for scams through retrograde amendments to the ePayments Code.**
- **Rules which provide for consumer refunds for scam losses need to be reformed to meet international standards.**

Losses from scams reach $2b/year

The ACCC now estimates that around $2 billion is lost in Australia a year on scams.[1] This follows scam losses increasing 84 percent in 2021 from the prior year.

Losses of this amount should be considered a national security threat and of macro-economic concern. $2 billion a year being siphoned to fraudsters will impede economic recovery following COVID-19.

Global figures, however, hide the impact that scam losses can have on individuals and families—the amounts lost individually can be life-changing.

Review of AFCA determinations

Analysis of ombudsman decisions

In February 2022, we undertook an analysis of AFCA determinations relating to scams. We searched the public database of determinations between 1 September 2021 and 1 February 2022 using the search term "scam". After some non-scam matters were excluded, we identified and reviewed 67 determinations. Out of these determinations:

- 62 were in favour of the bank or firm.
- Only 5 were in favour of the consumer.
- Scam losses complained of in these determinations amounted to $10,511,896.
- Consumer refunds in these matters (including non-financial loss) amounted to $706,313.
- This equates to only 6.72% returns compared to losses complained about

Matters not proceeding to determination

Our analysis could not cover AFCA matters resolved prior to determination, as there isn't transparency around these matters. There are, of course, many more complaints beyond those that proceed to determination. We understand that AFCA recommendations are made ordering a refund to a scam victim, and that banks do follow some recommendations.

Casework experience of matters that resolve prior to AFCA determination indicate that some banks make "low-ball" offers which result in consumers not proceeding with their complaint.

CASE STUDY

A 45-year-old woman named Arla contacted us in January 2022, experiencing anxiety and distress after her interactions with her bank. Arla received a phone call posing as Amazon stating that she owed $39.99 due to Prime service – she says that she had lost her dog that day, so had 'cloudy thinking' and experienced anxiety. Scammers asked her to go into her bank account, download an app, which let the scammer have control of the screen.

[1] Senate Economics Committee, Estimates, 17 February 2022

Phone 03 9670 5088 | info@consumeraction.org.au

CASE STUDY, cont.

Arlo thought this was required to resolve the Amazon issue. She provided them with three codes, which enabled the scammers to withdraw just under $12,000 from her savings account Arlo advised us that she had a $1,000 daily transaction limit, and that these transactions were uncharacteristic of her account use. Arlo rang the bank fraud line immediately. The bank told her they'd investigate but she'd be unlikely to have her money returned. The bank has now offered her $5,000 as a 'goodwill gesture'.

Themes from our analysis

Our analysis of the AFCA scam determinations identified the following themes:

1. In scam determinations (particularly investment scams), AFCA regularly begins determinations with the statement "there is no duty on banks to monitor account for fraud". There is commonly little analysis about the duties banks do have to identify red flags and when banks should query a mandate. Obligations on banks to take care in identifying and protecting against scams can arise from the following:
    - Implied warranties in a customer-firm contract impose a duty to exercise due care and skill.[2] In a UK decision, it was stated in relation to a duty of care on bankers that 'the law should guard against the facilitation of fraud, and exact a reasonable standard of care in order to combat fraud and protect bank customers and innocent third parties'.[3]
    - Banks regulated by AUSTRAC are required to monitor customer transactions, including unusually large transactions, complex transactions and unexpected patterns of transaction that do not seem to have a legitimate purpose. The primary purpose of these obligations is to protect against criminal activity, which includes fraudulent scam activity.
    - The obligation on firms to conduct services 'efficiently, honestly and fairly'[4] has been given more emphasis since the Banking Royal Commission. It is more efficient and fairer for banks to invest in capabilities to identify fraud risk compared to placing the onus on consumers. In 2020, ASIC initiated proceedings against a firm for failing to put adequate cyber security controls in place to protect customers as a breach of this provision.[5]
    - The Code of Banking Practice, including the promise to engage in a fair, reasonable and ethical manner, and the Australian Banking Association industry guideline, 'Protecting vulnerable customers from financial abuse' are also relevant instruments. The 2016 guideline confirms that pressuring a person to engage in financial scams is a form of financial abuse.[6] The AFCA Approach to Financial Elder Abuse similarly confirms that scams and illegal activity fall under the 'financial abuse' definition.[7]
    - Banks may also face liability to account to a scammed customer where the bank has knowledge of undue influence applied to a customer which prevents the customer from making a genuine and free choice regarding the transaction.[8] This can be observed from call recordings between banks and customers.
2. Banks often provide specific warnings of risky/potential scam transactions by contacting customers ahead of the transaction proceeding, but then proceed with the transaction in any event if the customer consents to the transaction proceeding. In these circumstances, banks sometimes ask "Do you accept the risk of this transfer"?

[2] Section 12 ED, ASIC Act 2001.

[3] *Barclays Bank plc v Quincecre Ltd* [1992] 4 All ER 363 at 376. See also *Territory Sheet Metal v ANZ* [2009] NTSC 31 at [1197 - 1217] for discussion about where duty means a bank should over-ride customer's mandate

[4] Section 912A(1)(a), Corporations Act.

[5] See https://download.asic.gov.au/media/5760712/20-191mr-concise-statement-asic-v-ri-advice.pdf

[6] ABA, Protecting vulnerable customers from financial abuse – Industry Guideline, 2016

[7] See: https://www.afca.org.au/what-to-expect/how-we-make-decisions/afca-approaches.

[8] See *RBS v Etridge (no 2)* [2002] AC 773 at 794-797, 802; *Thorne v Kennedy* (2017) 263 CLR 85 at [34].

Banks should consider the that the person being scammed is acting under 'undue influence' and is not able to consent to the transaction. Questioning whether the customer is willing to accept the risk of the transaction is meaningless, particularly where the customer has demonstrated limited capacity to understand the nature and implications of the transaction, and this is known to the bank.[9]

While this is a difficult issue, there are a large majority of investment scam determinations that fit in this category. The consumer's view inevitably changes when they realise that they are being scammed.

If banks are aware that the transaction is likely to be a scam, but proceed in any event, it may be considered that they are facilitating fraud to be perpetuated with knowledge.

3. The analysis identified examples of banks allowing customers to increase daily transfer limits without asking questions.

   Given the significant risk of increases or changes to daily limits being fraud-related, we would expect banks to take steps to prevent the customer from being scammed. Some banks do require a phone call discussion before transaction limits are increased and, as such, this would seem to define good practice.

4. Remote-access scams, where the scammer takes control of the consumer's computer and installs malware, are common. This is one scam where AFCA may consider the transaction to be unauthorised, and thus the consumer is not liable.

   However, the analysis identified inconsistencies in outcomes based upon ePayments Code rules regarding the sharing of pass codes. Where a complainant does not disclose their passcode, but enters it themselves, they are able to obtain a refund (that is, they did not share their passcode in line with ePayments Code liability rules). But where a complainant provides their passcode to a scammer (or scammer obtains it), then they are not eligible for a refund.

   This is an inconsistent outcome where consumers have been exploited by the same type of scam. Furthermore, it is unfair to say that the consumer is actively sharing passcode as they are acting under the control of a scammer (undue influence).

   It is worth noting that banks encourage their customers to share passcodes through 'screen scraping' processes common in loan applications, dulling the message to never share your passcode.

A better approach

AFCA should update its approach to scam complaints to better articulate the circumstances where it is appropriate for a bank to question a customer's instruction to make a transaction, including considering:

- The size of the transaction
- The transaction being significantly out of pattern with usual transactions
- The jurisdictions transfers are being made to is known for scams
- The vulnerability of the customer, e.g. age or disability
- The customer contacting their bank to increase their transfer limit
- The customer seems unclear about the purpose of transfers
- The customer is receiving instructions from a third party

If these circumstances are present, a bank exercising reasonable care and skill would enquire about the purpose of the transaction by making meaningful enquiries about the transfer, and not proceed with the transfer until they are reasonably satisfied that the transaction is not fraudulent.

We understand AFCA will be developing an "Approach to Scams" document in 2022, and we look forward to contributing.

ASIC reduces ePayments Code consumer protection

ASIC is proposing changes to the ePayments Code that will reduce consumer protection relating to scams.

[9] The customer cannot accept the risk because their understanding of that risk is markedly different to the bank's understanding. See *Vanker v Commercial Banking Co of NSW* (1972) NSWLR 967 at 975-76 where held that if both a bank and customer have been negligent, the bank will be held liable (concerned forged cheques presented by an associate of a very vulnerable consumer).

Consumer groups have made submissions[10] opposing the following proposals:

- That the definition of 'mistaken internet payment' be amended to ensure it only covers actual mistakes inputting the account identifier and does not extend to payments made as a result of scams.
- That the unauthorised transactions provisions only apply where a transaction on a consumer's account without the consumer's consent and do not apply where the consumer has made the transaction themselves as a result of falling victim to a scam.

Mistaken payments

The mistaken payment provisions of the ePayments Code require banks to take steps to seek return of payments made mistakenly and provide warnings on internet banking websites. Cases at AFCA confirm that these provisions do apply in scam situations (such as invoice hacking scams), and can operate to provide the consumer a refund where the bank has not met the standard in the ePayments Code.[11]

Removing their application to scam transactions will mean that consumers have no clear rights if banks do not take sufficient action to recover scam losses made through internet banking.

Unauthorised transactions

The ePayments Code confirms that consumers are not liable for transactions unless they are authorised.

Where a consumer is tricked into authorising a payment to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer, it is arguable that it is not authorised. For example, in romance or investments scams, the fraud generally arises following a relationship built on trust. The scammer grooms the consumer, and based on trust that develops, exploits the use of funds of the consumer. In these circumstances, the consumer was acting under the undue influence of the scammer and did not truly authorise the transaction for the purpose they believed it to be for.

ASIC's proposal to amend the code will mean that it will not apply in the above circumstance and will only apply where the scammer themselves fraudulently accessed the customer's account or card to initiate the payment. This is a backward step in terms of consumer protection.

Falling behind international best practice

In 2019, the UK introduced a voluntary industry code called the *Contingent Reimbursement Model Code for Authorised Push Payment Scams* (the CRM Code). 'Authorised push payments' is a term used in the UK to describe a range of scams where the customer is tricked into authorising a payment to an account that they believe belongs to a legitimate payee, but is in fact controlled by a criminal.

The CRM Code includes a fundamental principle that when a customer has been the victim of a relevant scam, the bank should reimburse the customer. There are some exceptions – for example, where the customer has ignored effective warnings (they were grossly negligent) – however, reimbursement is required (regardless of exceptions) where the victim is assessed as being vulnerable to scams.

A recent review of the CRM Code found that average reimbursement rates have risen from around 20% to 45% and banks have invested more heavily in warnings on their apps an online banking systems. Some institutions have introduced (either voluntarily or after being directed by the regulator) systems such as Confirmation of Payee to help people spot when they may be making a payment to the wrong account.[12]

Perhaps the most significant responses to the CRM Code have been at a systems level, with banks incentivised to improve real-time detection of online scam attempts. This includes the ability to flag and hold transactions pending investigation, and to refuse to process transactions unless the bank is satisfied that no fraud is present.

There is currently a proposal in the UK to make the CRM Code mandatory for all banks and payment systems providers.[13] This will, in effect, harmonise protection for

[10] Consumers' Federation of Australia, submission to ePayments Code review, June 2021, available at http://consumersfederation.org.au/wp-content/uploads/2020/08/210629-Submission-CP341-epayments-code.pdf

[11] See AFCA case 656981.

[12] Which?, The CRM Code: two years on, May 2021, available at: https://conversation.which.co.uk/scams/contingent-reimbursement-model-code-two-year-anniversary/

[13] See House of Commons Treasury Committee, Economic Crime Report, 2 February 2022,

'authorised' and 'unauthorised' transactions to incentivise banks to mitigate the risk of losses. Where accounts are accessed unauthorised (like card skimming, or card-not-present fraud), consumers are entitled to a refund. There is a need to be consistent where scams are 'authorised'.

While banks were given a chance to make necessary system changes through the voluntary code, it's now recognised that not all banks did—hence the move to a mandatory code.

Reimbursing scam victims will aid scam prevention

UK bank TSB provides a "Fraud Refund Guarantee" to its customers.

This means that if a customer is an innocent victim of fraud on their account, TSB will refund the money lost from the account. This includes where a customer has been tricked into making a transaction.

TSB has confirmed that this approach has supported customers in protecting themselves against scams:

> *"Our customers can better protect themselves in the future and [the guarantee] also allows us to gather better and more detailed information to continuously improve our fraud defences for the benefit of all customers. This insight is invaluable to TSB and we find our customers offer us more and better information on the types of scams that they have fallen victim to, because they know we will refund them. This means we can better protect against scams in the future and share relevant, timely and valuable intelligence with law enforcement and government."*[14]

This quote also confirms that bank concerns about 'moral hazard' (where victims would proceed with risky transactions aware that they will be refunded for any scam losses) are ill-founded. TSB state that where customers know they will be protected, they take steps to better protect themselves, and TSB is also in a better position to protect against scams in the future.

Further information

Further information about Consumer Action is found at www.consumeraction.org.au.

info@consumeraction.org.au
03 9670 5088

https://publications.parliament.uk/pa/cm5802/cmselect/cmtreasy/145/summary.html; and Payment Systems Regulator, APP scams consultation papers, November 2021, available at https://www.psr.org.uk/publications/consultations/cp21-10-app-scams/

[14] See: https://committees.parliament.uk/writtenevidence/18464/pdf/