Parliamentary joint Committee on Corporations and Financial Services

Oversight of ASIC, the Takeovers Panel and the Corporations Legislation, 20 October 2023

Australian Financial Complaints Authority

QoN no. 4

CHAIR: I'm also concerned about the intersection of scams with banks. They often get dealt with in separate sections and different conversations, but people's money is being removed from their banks. Largely it's an electronic transfer that's occurring. I'd like you to provide the committee with your insights into the intersection between those two things, what is being done, who is responsible.

Page 16 Hansard record

Answer

As noted in our appearance before the Committee, AFCA continues to see a significant increase in scam complaints. In the financial year ended 30 June 2023, AFCA received 6,048 scam complaints a 46% increase on the previous year. In the first quarter of FY24 there were 2,856 scam complaints received, up 57% from 1,819 last quarter, and 125% higher than the same period last year.

Our data show us the big four banks receive the greatest volume of scams. However, some of the second-tier banks seem to have a larger proportion of scam complaints compared to the volume of transactions they would process.

Further, AFCA only sees a fraction of scam complaints. We know from the work of the ACCC's ScamWatch and from our engagement with consumer advocates that many people do not complain.

AFCA is deeply concerned about the increase in scam complaints, the increasing sophistication of scams and the losses caused by them. We see first-hand the human cost of this serious financial crime. The impact of a scam on a person can be devastating and life changing.

We strongly support the Government's proposal for mandatory and enforceable codes of practice with clear standards that lift the bar for prevention and remediation of

scams and clear lines of liability, that would also aid the work AFCA does as an ombudsman service.

Although some positive steps have been taken by major banks, more is needed to address the scourge of scams and we would like to see a more consistent approach across the whole sector.

Banks have pushed people onto digital channels, and this has been exacerbated by branch closures, particularly in remote areas. In these circumstances, Banks need to make sure their products are accessible and safe to use by older and less digitally savvy customers.

Our interactions with scam victims show they can get different outcomes from different banks and even within different areas of the same bank. Banks often provide an ex-gratia payment, but they bear little relationship to the sum lost. Customers find it very difficult to understand the basis on which the Banks decide to give these amounts and how the amount itself is calculated.

We encourage all banks to consider what further steps they can take. Below we share insights on what banks and others are doing internationally, and steps banks can take here in Australia.

With scammers becoming increasingly sophisticated, organisations from across different industries will also need to work together to combat scams and educate the community.

Main Scam Types

The main types of scams that we see are set out below. Scams continue to evolve though and are becoming increasingly sophisticated.

Investment scams- are the main scam type that AFCA sees, and they often result in the loss of large sums of money including from Self-Managed Superannuation Funds (SMSFs). These often involve transfers of funds to crypto platforms.

Impersonation scams- where the scammer impersonates a person in authority such as bank officers, the ATO, service providers or large retailers. Recently it is generally bank officers being impersonated. These scammers employ tactics to convince the person they are dealing with their bank such as asking them to check the number they are calling from against the number on their card.

Romance scams- not as common but often involve large sums of money often over a number of months and tend to impact vulnerable people.

Seller/Buyer scams- these are often low value, but we do see some where large sums have been lost. The scam types referred to above often involve Phishing, ID spoofing and remote access. What we find is often old scams recycled with a new twist.

Email compromise scams- although these can involve consumers, they are the main scam type impacting small business complainants. The sums lost are often very large such as the proceeds of a property sale.

Superannuation scams- at the moment we see relatively low numbers. These numbers do not include the claims where we have seen funds lost by self-managed super funds in investment scams, which are picked up in the general scam data. We expect to see an increase in scams in relation to Superannuation given the large sums of money available in these accounts.

The types of scams we see in superannuation include rollovers to a non-existent fund, a superannuation account controlled by the scammer, identity theft or alleged hacking of the complainant's My Gov account.

Limits on AFCA's jurisdiction

AFCA does not have jurisdiction to deal with all the scam complaints that are lodged with it.

AFCA does not currently have jurisdiction to look at the actions of the receiving bank. This includes where the receiving bank processes may have facilitated the opening of a mule account.

In the UK for example, the Financial Ombudsman Service can look at the conduct of the receiving bank as a result of a change in its rules in Jan 2019. With the introduction of the Contingent Reimbursement Model (CRM) Code in the UK, the receiving bank must share liability with the sending bank in certain circumstances.

AFCA cannot consider claims where an account is opened using stolen identification documents. This is because the person impacted did not receive a financial service or does not have a customer relationship with the bank.

Limitations with regulation and codes

When considering Scam complaints, we look to see if the disputed transactions are unauthorised. Then if person scammed is a consumer and if the bank is an ePayments Code subscriber, we consider liability under the provisions of the ePayments Code.

Our cases show that there are limited avenues for recovery under the ePayments Code given the current definition of unauthorised transactions. The new ePayments Code that took effect from 2 June 2022 clarified the definition of unauthorised transaction as one that is not made by the customer or with their knowledge and consent. This definition means that payments made by a person or by the scammer with the customer's knowledge are treated as authorised payments even though clearly the customer did not intend to pay a scammer or a mule account.

When the Code was being finalised, ASIC acknowledged that it was not intended to cover scams. We note the Code does not apply to small business. It applies to

consumers where a transaction is performed wholly or predominately for personal domestic or household purposes.

The Code is voluntary, and some large players are not subscribers. It also does not consider technology such as tokenisation and digital cards/wallets. All these reasons make it difficult for a scam victim to be able to recover under the ePayments Code.

Legal Limitations

The current legal position is unclear and there are several areas where there are no obligations on financial firms except for the general conduct obligations under section 912A of the Corporations Act and the Banking Code of Practice.

These do not go far enough or offer sufficient protection. The following illustrate gaps in the current legislation and common law.

Authorised transactions

Complainants that make authorised pay anyone transactions online or in branch, generally have no basis for recovery under current law and codes unless it can be shown the bank has done something wrong.

Recall

There are no obligations on bank's regarding recall outside of the mistaken internet payment obligations. This means there is no time frame to lodge or get a response on a recall request. There is also no requirement to keep the customer up to date on the progress of any recall.

Excessive wait times

There are no obligations around having efficient and timely means for customer to report scams and get help during a scam. We have had claims where customers have reported trying to get through to bank fraud departments for forty-five minutes to one and a half hours. One customer attended the branch and was told to go home and try again as branch staff would not be able to get through any faster. There needs to be an ability to report scams quickly so banks can act including by holding or stopping payments.

We note that in Singapore since January 2022 there is a requirement for financial firms to have dedicated and well-resourced customer assistance teams to deal with feedback on potential fraud cases on a priority basis.

From June 2022 in Singapore to facilitate rapid account freezing and fund recovery operations bank staff and law enforcement staff have been co-located at their Anti-Scam Centre.

From June 2023 Malaysia banks must have a 24/7 dedicated complaint channel for customers. In the UK, the Banking Protocol, an initiative by UK Finance in partnership with National Trading Standards, trains bank branch staff to spot when someone is about to fall victim to a scam and to try and prevent them from withdrawing cash to give to a fraudster. Staff can request an immediate police response to the branch to investigate the suspected fraud and catch those responsible.

Five critical changes that would disrupt or prevent scams

Our complaints and information sharing with overseas ombudsman services indicate that the following five changes would greatly disrupt and prevent scams, and banks and others should consider how these can be adopted here in Australia: -

1. Confirmation of Payee

- In Australia payments through the Bulk Electronic Clearing System only matches BSB and account numbers. This facilitates scam payments where the account name provided by the scammer differs from the real account name. This occurs in email compromise scams and in some investment and buying and selling scams.
- As highlighted above, some of the big banks are using their data to predict the likelihood of the account being held by the entity named.
- CBA introduced Name Check in February this year. Due to volume of transactions, it has been able to use its own data to predict the chance of a first-time payment going to the named account. For example, if it has seen several payments to the account and no complaints, it says there is a high chance the account is owned by the entity named as account holder.
- Westpac has used the same technology to launch their version Verify, using a similar process.
- At this time, it does not appear other Banks are adopting the name checks technology.
- Confirmation of payee is the major weapon against invoice hacking scams and many impersonation scams.
- In the UK confirmation of account name BSB and account number is now mandatory for the major banks (since 2020) and in October 2022 it was announced it will expand to 400 other banks and financial firms. The first tranche was due to be compliant by October 2023 and the remainder by October 2024. Confirmation of payee is also available across a lot of Europe.

2. More secure delivery of codes (OTPs) and communication- removing links

- Many scams involve the scammer asking the person to provide codes that are sent by the financial firm to approve a new payee, transaction or some other purpose. Often the scammer can convince the person the code to perform a transaction is for a purpose other than to perform a transaction. Where the scammer has remote access of a mobile device the OTPs can be received by the scammer and deleted without the person knowing they have received them.

- Financial firms could move away from links and codes delivered by SMS. NAB announced in July it would remove links in SMSs. ANZ and CBA have said they will follow. This has been mandated in Singapore since January 2022 for retail customers.
- Codes should be delivered in banking apps, or a new method of authentication other than codes should be devised.
- In Malaysia from 22 June 2023, they have migrated from SMS one-time passwords (OTP) to a more secure in app authentication method.
- Also, when a bank calls, the bank officer can ask the customer to go into their banking app, view a message and thereby receive validation it is the bank calling. We understand CBA is doing something like this.

3. Customer Empowerment and further authentication

- Empowering customers by giving them the ability to control access to their banking products and limits. For example, customers can opt for limited access methods to accounts.
- Various limits for different payment services such as pay anyone, BPay etc should be more transparent and customer driven. Customers should be informed of default limits and be able to lower limits on various payment methods easily. There should be lower default limits particularly for debit cards. Limit increases should require additional authentication.
- Ability for customers to freeze or lock their own accounts if they are worried about third parties accessing the account or feel they have made a payment to a scammer. This could also be done if customers know they will not be requiring access to a particular account for a period while for example they are away.
- In Singapore from June 2022 Banks have an in-banking app emergency self-service “kill switch” for customers to suspend their accounts quickly if they suspect their bank accounts have been compromised.
- Further authentication required if a customer seeks to set up internet banking or access internet banking on a new device, add a digital card to a wallet on a new device or change their internet banking passcode.
- In Malaysia since June 2023, they have had verification and a cooling-off period for first time enrolment of e-banking services.
- In Singapore since January 2022 there is a cooling-off period before implementation of requests for key account changes such as customer contact details.
- There is also notification to the existing mobile number or email registered with the bank when there is a request to change a customer’s mobile number or email.
- Since January 2022 Singapore has had a delay of at least 12 hours before activation of new soft token on a mobile device.
- In Malaysia from June 2023 a digital card can only be added to a single mobile device.
- We note a couple of the major banks are looking at implementing additional authentication measures around digital cards.

4. Restrictions on Crypto

- Cryptocurrency scams are one of the biggest scam types. Funds can be channelled through a legitimate crypto platform, or the scammer convinces the person to provide details of their crypto account/ wallet and takes the funds from the account /wallet.
- We think it imperative that restrictions, delay and friction be considered for crypto transfers.
- In the UK, every bank has acted because of the reversal of the onus of proof to introduce friction into payments to crypto platforms. TSB Banking Services in the UK which offers a fraud refund guarantee does not allow payments to crypto platforms.
- Given the large number of scams involving crypto we think it would make sense to introduce measure such as a 24 hour hold on first payments to a crypto platform, or a dollar limit per payment or period, which could be changed if customer contact the branch.
- Credit cards should not be able to be used to purchase crypto. Just like some of the restrictions on the use of credit cards for gambling.
- From May 2023 Westpac blocked payments to Binance and other crypto platforms it has designated high risk.
- From 8 June 2023 CBA made changes to decline or hold on certain payments to crypto exchanges. Blocked exchanges with high scam activity.
- CBA has changed its terms and conditions so no more than $10,000 can be sent to a crypto exchange in a month.
- NAB announced on 7 July 2023 that it will no longer send funds to certain crypto platforms. Also, it will be implementing a 24-hour hold for first time payments and monthly limits to crypto platforms.
- ANZ has indicated it will also be blocking certain high-risk payments to crypto platforms. It may hold first time payments for 72 hours.
- Singapore has banned payments to crypto platforms for retail customers.

5. Recall and liability of the receiving bank (mule accounts)

- The ePayments Code sets out a regime for banks to recall funds mistaken internet payments. Mistaken internet payments are where a person makes a typo in the BSB or account number or selects the wrong account from a drop-down box. The ePayments Code prescribes time frames in which requests must be made and when repayments can be made. It also places obligations on the receiving bank around recall.
- Credit card scheme rules have charge back codes that can be used to reverse payments.
- For pay anyone and other type of payments there are no recall obligations and rules about when funds can be taken from the recipient's account.

- The receiving bank does not have any obligation to respond in a particular time frame or manner for pay anyone scams. The receiving bank often refuses to provide information to the sending bank because of Privacy or confidentiality.
- In the UK, the new legislation provides that the liability for a scam will be shared 50% by the sending and receiving bank.
- The scam could not occur without the ability to open and obtain mule accounts.
- When opening accounts, the bank should check the person providing the ID is the owner of the ID- no exceptions for online account opening.
- Crack down on people allowing accounts to be used as mule accounts for a fee.
- Crack down on people involved in purchase and sale of bank accounts that can then be used as mule accounts.
- Obviously live data sharing particularly around mule accounts will be invaluable. We have met with the Australian Financial Crimes Exchange and look forward to the expansion of their data sharing activities across industry and the possibility of preventing scams and fraud real time.