26 March 2021

The Director
AFCA Review Secretariat
Financial System Division
Treasury
Langton Cres
Parkes ACT 2600

Via email: AFCAreview@treasury.gov.au

Dear Director

Treasury's review of the Australian Financial Complaints Authority

COBA appreciates the opportunity to contribute to Treasury's review of the Australian Financial Complaints Authority (AFCA).

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $146 billion in assets, 10 per cent of the household deposits market and more than 4.5 million customers. Customer owned banking institutions deliver competition, choice and market-leading levels of customer satisfaction in the retail banking market. Our members range in size from less than $200 million in assets to around $15 billion in assets.

All COBA members are AFCA members.

COBA members' point of difference is our ownership model – our customers are also the owners of our institutions. This model removes the motive to undertake the 'profit before people' behaviour examined in the recent Banking Royal Commission. Our model better aligns the incentives of customers and their bank and reduces the risk that the bank's purpose will create demand for external dispute resolution.

In addition to the pro-consumer bias of our model, key promises made to customers by subscribers to the Customer Owned Banking Code of Practice include:

- We will be fair and ethical in our dealings with you.
- Will focus on our customers.
- We will be responsible lenders.
- We will deliver high customer service and standards.
- We will deal fairly with any complaints.

COBA's submission covers questions one, three and four of Treasury's terms of reference. We have also attached our recent submission to AFCA in response to a draft factsheet provided to COBA by AFCA about scams and AFCA's approach to complaints about scams.

Key points

- **AFCA should demonstrate a stronger commitment to impartiality between complainants and AFCA member firms and to give appropriate weight in AFCA determinations to the obligations and responsibilities of complainants.**

- **AFCA should publish indicative timeframes for the various phases of dispute resolution and demonstrate a commitment to meet these timeframes in most cases.**
- **COBA members need more clarity about AFCA's internal processes and procedures in case management and decision-making to address concerns about the variability of outcomes and lack of attention to the importance of precedent.**
- **The structure and scale of AFCA's member levies, user fees and complaint fees should be improved to address concerns about fairness, efficiency and the quality of decision-making and dispute handling processes.**
- **COBA members support AFCA having an internal mechanism to review the substance of decisions in prescribed circumstances. The monetary jurisdiction of AFCA is considerable and there is a need for additional assurance to be provided by an appropriate review mechanism to promote confidence in AFCA's performance.**

Delivering against statutory objectives

Is AFCA meeting its statutory objective of resolving complaints in a way that is fair, efficient, timely and independent?

COBA and its members have a strong working relationship with AFCA and we appreciate AFCA's willingness to engage proactively with industry to develop better information sharing and ultimately improve outcomes for both consumers and financial institutions.

Overall, COBA members have varied experiences with AFCA, both with respect to their interactions and the outcomes received throughout the dispute resolution and determination process. Many members have reported their engagement with AFCA to be positive and constructive in many instances leading to a resolution of consumer complaints in a fair, efficient and timely manner.

However, member feedback also indicates concerns about AFCA with respect to fairness, efficiency and timeliness, based on their interactions throughout the dispute resolution process.

Fair and independent

AFCA is required by legislation to operate in a way that is accessible, independent, fair, accountable, efficient and effective.[1]

Fairness requires complaints to be considered objectively and without bias, and by AFCA staff and decision makers with appropriate expertise.[2]

Broadly, COBA members considered AFCA to be fair and independent in most instances.

Some members have highlighted the challenges that AFCA faces in balancing its role as the independent assessor of disputes versus assisting individual complainants

Members have provided consistent feedback to COBA that AFCA's interpretation of its fairness mandate can sometimes lean towards customer advocacy. Members would like to see AFCA demonstrate a stronger commitment to impartiality between complainants and AFCA member firms.

COBA member concerns about fairness were most frequently reported in the context of AFCA's handling of complaints involving scams. Various COBA members reported issues with AFCA determinations in scam complaints where the financial institution has been held liable for consumer financial loss despite financial institutions undertaking a wide range of measures and warnings to protect the consumer.

[1] https://www.afca.org.au/about-afca/fairness

[2] https://www.afca.org.au/about-afca/fairness

Members are concerned that AFCA's approach in some of these cases could undermine long-standing obligations on consumers to take care not to expose themselves to loss. One such case involved the victim allowing an external party to gain access to the victim's computer and subsequently the scammer obtained a secret code, enabling the external party to transfer funds from the victim's account.

AFCA's determination in this case said:

> *While the complainant's recollection is at times unclear, there is enough information to show that more likely than not:*
>
> - *He genuinely thought he was dealing with a telecoms company providing a computer maintenance service at the time*
> - *The third party gained access to his internet banking without his knowledge or consent*
> - *Even accepting he provided the [one time password] to the third party, he did not voluntarily disclose the internet banking password given the fraudulent access to his computer.*
>
> *Consequently, he cannot be held to have voluntarily disclosed the internet banking password at the least. This means under section 11.3 of the ePayments Code he is not liable for the disputed transaction.*[3]

Allocating full liability for the loss to the financial firm in this case appears to be an unfair outcome for the firm and undermines the firm's confidence in AFCA. More broadly, the determination sends the wrong signal to consumers about the need to be careful and vigilant to avoid becoming the victim of a scam.

AFCA's approach in cases like this does not given enough weight to individual accountability and the obligations and responsibilities of consumers.

For a customer owned bank, the cost of being made liable for a loss by one customer is borne by all customers as owners of the bank.

Efficient and timely

Efficiency and timeliness of AFCA in resolving disputes was also raised as a key concern by COBA members. While members reported that some matters are dealt with efficiently, there are a number of matters which have taken considerable time and resources to resolve, in turn imposing additional costs on COBA members.

While AFCA seeks to provide some timeframes regarding the dispute resolution process, specifically throughout the registration and referral stage, these obligations are more focused on addressing the timelines of the financial institutions, and not the AFCA representatives.

As it stands, neither consumers nor financial firms have the right to timely decisions by AFCA, despite this being an underlying principle of the regime's operation.

In some cases, once the registration and referral stages have been completed, COBA members have faced months of delay in AFCA allocating case managers to undertake the substantive dispute resolution.

Some COBA members have had matters running longer than 12 months, with one member reporting a case that remains unresolved after more than 650 days.

[3] AFCA determination 606063, https://service02.afca.org.au/CaseFiles/FOSSIC/606063.pdf

In another case, a COBA member had an ongoing matter before AFCA which was referred from the preliminary assessment stage through to determination in October 2020. As of 10 March 2021, five months later, the member was yet to receive any determination or communication about the decision.

It would be helpful to the objective of more timely and efficient resolution of disputes for AFCA to publish indicative timeframes for the various phases of dispute resolution and to demonstrate a commitment to meet these timeframes in most cases. While COBA notes that matters vary in complexity, indicative timeframes and the related commitment would allow both consumers and financial institutions to have more clarity and certainty in how the AFCA process will play out and save resources for financial institutions by helping reduce the incidence of protracted disputes.

Is AFCA's dispute resolution approach and capability producing consistent, predictable and quality outcomes?

COBA members reported moderate levels of satisfaction with AFCA's approach to dispute resolution, noting an improvement in their dealings with AFCA since its inception. Members recognised the efforts AFCA is undertaking to increase staff and resources and bolster their internal capabilities.

However, a significant theme in feedback from COBA members was concern about the consistency and predictability of outcomes. There were also some concerns regarding the quality of the outcomes reached in AFCA's approach.

Consistent and predictable outcomes

AFCA's decisions must fairly reflect the information provided to the parties and the application of the decision-making criteria in the Rules. Recognising that consideration of each complaint must take into account its particular facts, AFCA is expected to achieve consistency in its decision making.[4]

Feedback from COBA members indicates there is widespread concern that AFCA is falling short in this objective.

Many COBA members would like more clarity about AFCA's internal processes and procedures in case management and their decisions. This is due to concerns about the variability of outcomes of matters they have had before AFCA and lack of attention to the importance of precedent.

Members also reported instances where case managers have changed several times if a matter is open for a long period of time, resulting in a lack of continuity for the matter and sometimes even a change of AFCA's view on key aspects.

The lack of consistency and predictability in AFCA's approach to dispute resolution creates the need for COBA members to devote more time and resources to the dispute resolution process, both in trying to understand and navigate AFCA's approach and in their own internal decision making about how to proceed with individual cases.

COBA members are supportive of more transparency from AFCA of their internal protocols and procedures when managing cases and making determinations, as well as AFCA's treatment of previous decisions as precedent.

Do AFCA's funding and fee structures impact competition? Are there enhancements to the funding model that should be considered by AFCA to alleviate any impacts on competition while balancing the need for a sustainable fee-for-service model?

[4] https://www.afca.org.au/about-afca/fairness

AFCA is funded by membership levies, user charges and complaints fees. All Australian financial firms must be members of AFCA by law and are required to pay a membership levy and other complaint-related charges to contribute to AFCA's operating cost.[5]

COBA is concerned about the disproportionate burden of AFCA's funding and fee structures and the adverse impact on competition.

Categorisation of business size for membership levy

The membership levy is the fee all financial firms have to pay to be a member of AFCA. The levy covers a financial year and the amount an individual member pays is determined by a range of factors, including the relative size of the member's business compared with other AFCA members.[6]

AFCA's 'very large' category comprises the four major banks, other major domestic banks and five of COBA's largest members. Within the 'very large' category, there is an enormous difference in the size and scale of banks, which pay the same membership fee.

For example, the total resident assets (TRA) held by the biggest bank within AFCA's 'very large' category (CBA) is 21 percent of the Australian market, with the next largest bank (Westpac) at 19.8 percent of the market.

Within the very large band for non-COBA members, the share of the total market for assets ranges from 21 percent to 3.59 percent.

The five COBA members which fall within the 'very large' bank category have between 0.42 and 0.21 percent of assets, meaning their market share of TRA is 2 percent of the largest bank within the 'very large' category.

Despite this discrepancy in size, these five COBA members are subject to the same membership levy as an institution with 50 times their assets. This is unfair and should be addressed by a change in the levy structure.

User charges

AFCA's user charge "is a fixed annual amount which is calculated and proportionately allocated to members annually, based on a range of factors. Members who have only one, or no, complaints closed in the relevant 12-month period do not incur a user charge. This approach rewards members who increase their IDR resolution rates and reduce the need for their customers to use AFCA."[7]

COBA members report they have little to no transparency about how the annual usage charge is calculated, other than that their user charge fee is based on the number of matters that are received and progress beyond the registration and referral stage.

Some COBA members have reported a dramatic increase in their annual user charge over the two full years of AFCA's operation. One COBA member's user charge rose from $1,210 for the first full year of AFCA's operation to $9,295 annually for the second year.

Because of the lack of transparency into the user charges calculation, the member has been unable to specifically identify why that charge increased so much. The member concluded that the increase was attributed to how many matters were taken to determination stage.

[5] https://www.afca.org.au/about-afca/corporate-information/funding

[6] https://www.afca.org.au/members/member-faq

[7] https://www.afca.org.au/members/member-faq

The lack of transparency around the user charge poses additional challenges to COBA members on the basis that they are not able to fully understand what is driving their AFCA costs up – and therefore are unable to address the cause of the problem.

Complaint fees

If AFCA receives a complaint against a firm, the firm is required to pay an individual complaint fee. AFCA's services are free of charge to consumers who make a complaint.[8]

"The complaint fee for a particular complaint is based on the stage in the process at which the complaint is resolved and the complexity of the complaint if it progresses beyond the initial investigation stage."[9]

While COBA supports a free external dispute resolution scheme for the resolution of consumer complaints, there is a need to manage the cost impact of situations where consumers are pursuing frivolous or vexatious complaints.

The current complaint fee system lacks any disincentive for consumers to repeatedly lodge claims with little to no merit or to unreasonably extend consideration of matters. This is because all the costs incurred throughout this process lay with the financial institution.

COBA suggests that consideration be given to a model where the complainant bears some cost if their case is determined to have no merit, such as at the preliminary assessment stage. Should the consumer wish to escalate the complaint, the complainant could be required to pay a fee to cover some of AFCA's costs. This could reduce frivolous or vexatious complaints, freeing up resources for AFCA to focus on other cases.

We do not have a view about quantum of the cost to be shared with the complainant but we expect it would be a nominal fee, rather than a fee based on cost recovery. The model could be designed to reduce risks of discouraging vulnerable consumers from pursuing their rights.

The objective of this suggestion is to reduce costs overall, ultimately benefiting all stakeholders.

Settlements based on cost assessment

Some COBA members report that AFCA's fee structure can discourage firms from ensuring matters are fully considered and resolved.

This can lead to matters of dubious merit being settled and therefore a lost opportunity to set a useful precedent.

Some COBA members report that the risk of incurring considerable user charges and complaint fees, coupled with the potential for an adverse decision by AFCA, and associated reputational impact, has led them to settle disputes where they feel they have met their obligations to the complainant.

This could create the perverse outcome of encouraging more consumers to take disputes of dubious merit to AFCA, hence increasing costs on AFCA members in the form of user charges and complaint fees. From a competition perspective, this could favour larger and better resourced financial firms over smaller firms, as they are better resourced to settle matters.

A COBA member has suggested considering a model whereby a reduced complaint fee is levied on a financial institution if AFCA finds no wrongdoing by the institution. This would encourage financial institutions to pursue matters that otherwise would not be economical to run and would also allow AFCA to set some good precedents in various factual scenarios.

[8] https://www.afca.org.au/about-afca/corporate-information/funding

[9] https://www.afca.org.au/members/member-faq

Potential enhancements to the funding model

COBA proposes consideration of the following proposed enhancements to the funding model:

- Greater transparency and recalibration of the 'business size' categories and associated fees to more accurately reflect the individual business' market share,
- Improved transparency on the calculation of user fees to give financial institutions a clearer picture of where they are accruing costs and allow for better budgeting, and
- The introduction of a disincentive for complainants to pursue matters that AFCA has determined to have no merit, to deter consumers from making repeated, frivolous or vexatious complaints.
- A reduced complaint fee for financial institutions if AFCA finds no wrongdoing by the institution.

Internal review mechanism

AFCA's Independent Assessor has the ability to review complaints about the standard of service provided by AFCA in resolving complaints. The Independent Assessor does not have the power to review the merits or substance of an AFCA decision.

Is the scope, remit and operation of AFCA's Independent Assessor function appropriate and effective?

Some COBA members had limited or no awareness of AFCA's independent assessor function. They viewed this lack of knowledge about the independent assessor as indicative that the function is not operating in a way that is appropriate or effective.

Members with knowledge of the independent assessor function indicated that its scope, remit and operation limits its effectiveness.

Members suggested that dissatisfaction with AFCA's dispute resolution outcomes are often due to the substance of cases or interpretation of the facts, which sit outside the independent assessor's terms of reference. The independent assessor's inability to review the substance of a case hinders the effectiveness of its operation.

COBA recommends that the independent assessor's function should be better communicated to financial institutions and consumers in order to increase its utility and improve dispute resolution outcomes.

Is there a need for AFCA to have an internal mechanism where the substance of its decision can be reviewed? How should any such mechanism operate to ensure that consumers and small businesses have access to timely decisions by AFCA?

COBA members support AFCA having an internal mechanism to review the substance of decisions in prescribed circumstances.

The monetary jurisdiction of AFCA is considerable and there is a need for additional assurance to be provided by an appropriate review mechanism to promote confidence in AFCA's performance.

Members suggested that the review mechanisms should be facilitated via an appeals process to a separate and independent team within AFCA. The team would have higher levels of expertise and understanding of banking and payments.

The introduction of a substance review function would have to carefully balance AFCA's imperative to resolve disputes in a quick and efficient manner. Members stressed that any review function should have prescribed time frames and not add further delays to what can be a lengthy AFCA dispute resolution process.

Members also noted that their support for an additional review mechanism would be subject to it having a reasonable cost dimension.

A substance review function could address the inconsistencies that are currently occurring under AFCA's current decision-making regime. It would also support members in instances where AFCA's position changes between the preliminary view and subsequent determination, by providing parties to the dispute with the opportunity to clarify AFCA's deliberations.

Members found the current test case regime to be unsatisfactory, as it requires AFCA permission to be run and allows AFCA to impose its chosen requirements upon the provision of permission. In addition, the limitation of review to 'test cases' does not address one-off poor decisions, the consequences of which can be significant given AFCA's monetary jurisdiction.

The requirement that financial institutions pay the costs of both parties in test cases is also a restraint, evidenced by the limited number of test cases run under the current arrangement. Members believed this to be driven by the costs incurred, rather than the high level of satisfaction with AFCA decisions.

Thank you for the opportunity to provide these comments. If you wish to discuss any aspect of this submission please contact Luke Lawler (llawler@coba.asn.au) or Maryanna Vasilareas (mvasilareas@coba.asn.au).

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer

ATTACHMENTS:

- ***AFCA draft factsheet on scams***
- ***COBA submission in response to AFCA draft factsheet on scams***

Factsheet - Scams

Scams affect all sectors of the Australian community and are becoming increasingly common. Scammers use a range of techniques to target people and steal their money. Scammers continue to develop new ways to defraud people.

People complain to AFCA about many different types of scams, including investment scams, romance scams, invoice hacking scams and remote access scams. In many cases, payments to scammers are made electronically.

AFCA can only consider complaints against financial firms who are our members. In most cases, the scammer is not an AFCA member and therefore we are unable to consider a complaint about their behaviour.

However, we can consider whether a financial firm should be liable for all or some of the losses suffered by the customer – for example, because the financial firm failed to take reasonable steps to prevent the loss in circumstances where it ought to have acted.

The purpose of this document

The purpose of this document is to inform the Australian community about:

- the sorts of complaints about scams AFCA commonly sees
- how AFCA approaches complaints about different types of scams

It is important to remember that complaints about scams can raise complex issues. The outcome of each complaint will depend on exactly what happened in that particular case.

Investment and romance scams

What are investment scams?

Investment scams are commonly spread by email and social media.

The scammer will usually invite the customer to click on a link about investing in shares, derivatives or digital currency so they can make money quickly.

Investment scammers will often promise huge returns like “double your money in two months” or “make $1 million fast using this secret technique”.

These scams will often use the names of well-known celebrities to make them appear genuine and credible.

The investment scammer will usually ask for the customer's contact details, then contact the customer directly to encourage them to set up a trading account on the scammer's preferred trading platform.

The scammer will usually persuade the customer to transfer money to the scammer or to the trading platform using their credit card or internet banking. Sometimes the scammer will pressure the customer to attend a branch to transfer the funds in person.

Usually, the scammer's online investment platform will show the investments performing well for months or even years. The scammer will use these fake profits to encourage the customer to transfer even more funds to the investment platform. Unfortunately, the customer may only learn the investment is a scam when the investment value shown in the trading platform suddenly reduces, or the scammer refuses to let the customer withdraw their funds.

What are romance scams?

Romance scams involve a scammer connecting with a customer over the internet through social media, email or an app. The scammer pretends to build a relationship with the customer, but the scammer's personality, pictures and identity are fake.

After the relationship has formed, the scammer then asks the customer to send funds to help them with living, travel or medical expenses. The scammer might pretend to be in trouble or lie about an emergency to pressure the customer to send them money. The first request may be for a small amount of money, then the scammer may start asking for more and more money over time.

Romance scams involve a strong element of emotion. It can be months and sometimes years before a customer realises the relationship was fictitious and they have been scammed.

Often the bank or the customer's family will notice what is happening and will try to tell the customer that they are being scammed, but they may not want to believe it.

How AFCA approaches investment and romance scams

When AFCA receives a complaint about an investment or romance scam, we always begin by considering if the customer authorised the transactions to transfer the money to the scammer. Usually, because of the deception involved in these scams, the customer authorised the transactions (i.e. made them themselves and intended to do so) but did not realise they were paying a scammer.

Where the transactions were made using an account held with a financial firm, such as a bank, AFCA will consider whether the financial firm met its obligation to the customer and whether it is required to compensate the customer for the funds lost by the scam.

The typical customer-financial firm relationship is one of customer and service provider. This means a financial firm, such as a bank, is ordinarily required to carry out its customers' instructions. Financial firms do not have a general obligation or duty of care to observe or monitor their customers' transactions, or to maintain watching briefs of scams for its customers' benefit.

However, financial firms do have some duties to customers under the law, applicable industry codes and general standards of good industry practice.

Financial firms cannot turn a 'blind eye' to warning signs

At law, a financial firm has a duty to act as a prudent and diligent banker. AFCA also expects financial firms to act in accordance with applicable industry codes and good banking practice. A financial firm cannot turn a 'blind eye' to warning signs that indicate their customer may be at a real risk of being scammed.

If a customer is scammed and complains to AFCA, we will consider if the Australian Securities and Investments Commission (ASIC) issued a warning notice to the financial firm about the recipient of the funds before the customer sent the funds. We expect financial firms to be aware of such warning notices and comply with them by blocking transfers to that scammer.

Where a customer makes a transfer in a branch, the financial firm should identify any warning signs that may indicate the customer is being scammed and make appropriate enquiries about why the customer is sending the money and who they are sending it to. A financial firm may also have an opportunity to identify warning signs if they have a telephone conversation with the customer (for example, if the customer calls to increase their daily transfer limit or the financial firm calls them because its fraud area flags a transaction as suspicious).

Warning signs may include:

- transactions that are outside the customer's usual spending habits (such as higher amounts and where a recipient is in a country the customer has not sent funds to before)
- transactions that are being sent to countries well known to be used by scammers
- any apparent vulnerabilities, such as age, known or readily apparent medical condition or disability[1]
- how the customer contacted the financial firm, such as the method or frequency of contact being out of the ordinary
- the behaviour of the customer when speaking with the financial firm such as:
  - being secretive or guarded about the purpose of the transfers, or

[1] AFCA has issued an approach document called "The AFCA Approach to financial elder abuse". The document is located on the AFCA publication page under AFCA Approaches. The document considers how to identify warning signs of financial elder abuse, considers what is good industry practice in response and discusses how AFCA assesses these complaints.

- talking to another person on the phone while giving instructions to the financial firm.

Where a bank identifies a warning sign it should make meaningful enquiries with the customer to see if they are being scammed by:

- finding out how the customer knows the recipient, whether they have met them in person or dealt with them before and whether they have researched their legitimacy
- whether the customer has discussed the transfer with a trusted family member, friend or financial adviser
- warning the customer about scams and the low likelihood of recovering the money if it is sent overseas and the recipient turns out to be a scammer
- asking for a document to show the purpose of the transaction, such as a share purchase agreement or an invoice.

The financial firm's inquiries should be meaningful, not just a 'tick a box' exercise. If the customer's answers are not clear, the financial firm should ask follow-up questions. If the customer still appears confused or is unable to reasonably show that the transaction is legitimate, it may be appropriate for the financial firm to refuse to process the transaction until it can be satisfied that the transaction is legitimate.

If a financial firm does not meet its obligations to act as a diligent and prudent banker, it may be required to compensate its customer for all or part of their loss. The compensation awarded will depend on the extent to which the financial firm's conduct has contributed to the loss.

Invoice hacking scams

What are invoice hacking scams?

An invoice hacking scam involves a scammer gaining access to the email account of a genuine business and changing the information on its invoices so that customers receiving the invoice mistakenly pay money to the scammer rather than the business. These scams often operate without the knowledge of either the customer or the business.

For example, a scammer may intercept a genuine invoice that a builder intends to email to their customer. The scammer could change the builder's account number and BSB on the invoice (but not the account name) to the scammer's account details. When the customer makes the payment as instructed by the hacked invoice, the money will go to the scammer rather than the builder.

How AFCA approaches invoice hacking scams – mistaken internet payment

If the customer made the payment online, it will usually fall within the definition of a mistaken internet payment (MIP) under the ePayments Code (Code). Usually, the customer authorised the payment (because they intended to make it), but they meant to pay the money to the legitimate business, not to the scammer.

The Code applies when individuals in Australia use electronic payment facilities to transfer money. It is a voluntary code and therefore does not bind financial firms who have not subscribed. The Code does not provide protection for small business customers.

However, AFCA considers the warning provisions about MIPs in the Code to be good industry practice. We expect all financial firms to comply with the warning requirements, including when dealing with small business accounts.

This means that all financial firms should display an onscreen warning when a customer authorises an electronic transfer advising that:

- the financial firm does not check the account name provided matches the account number or BSB of the payee account and the customer should carefully check these details (unless it does – AFCA is aware that some financial firms do check this), and
- the funds may be unable to be recovered if they are paid to the wrong account.

AFCA also expects financial firms who subscribe to the Code to follow the steps set out in the Code when a customer advises the financial firm that they have been the victim of an invoice hacking scam. These provisions require the financial firm to promptly notify the receiving financial firm of the MIP.

The receiving financial firm may need to return or freeze the funds. However, this will depend on:

- the time since the MIP was made, and
- whether the funds are still available in the recipient's account.

As the Code requires the sending and receiving financial firms to cooperate with each other, if it is apparent the receiving financial firm has not complied with its obligations under the Code, AFCA may require the sending financial firm to compensate the customer. However, AFCA:

- cannot consider a complaint by the customer who sent the funds against the receiving financial firm.
- can consider a complaint lodged by the intended recipient of the funds (the business that had its invoice hacked), against the receiving financial firm. We

would then consider if the receiving bank complied with its obligations to the intended recipient.

Even if the Code does not apply, we still expect financial firms to take steps to attempt to recall a mistaken payment sent from a customer's personal or small business account without delay.

How AFCA approaches invoice hacking scams – transaction made at a branch

Sometimes customers who are victims of an invoice hacking scam will go to their local branch to make the transfer. While the Code does not apply, AFCA considers it good industry practice for the bank to warn the customer that:

- it will not consider the account name when processing the payment, so the customer must carefully check the account name and details provided
- if the customer does not do this, then they risk paying funds to the wrong account and the funds may not be able to be recovered.

The financial firm may adequately warn its customer by including a warning **prominently** on the transfer form, such as on the front page above the customer's signature or drawing the customer's attention to a warning in the terms and conditions on the form and asking the customer to sign next to the relevant term.

If the financial firm does not give this warning, then the account name provided by the customer forms part of the financial firm's mandate. This means the financial firm will not be following its customer's instructions if it processes a payment to the scammer's account using the BSB and account number where the scammer's account has a different name. AFCA may find the financial firm is liable for loss resulting from the transaction on this basis.

Recall requests and chargebacks

There are some methods a bank can use to try to recover funds that a customer has sent to a scammer. These methods are not often successful, but we expect a bank to take reasonable steps to assist.

We expect a financial firm to initiate a recall request within two business days, if a customer tells their financial firm that they believe they have been scammed and asks the financial firm to try to recover the funds from the scammer. A recall request is where the sender's financial firm asks the recipient's financial firm to return the funds.

Recall requests are rarely successful when funds have been sent to a scammer. Often the scammer will remove the funds soon after receipt, so they are no longer available or will refuse to return the funds. In most circumstances, the receiving financial firm can only return the funds with their account holder's consent and a scammer will not give it.

A financial firm also has an obligation to raise a chargeback if the customer sent money to the scammer using a credit card and a valid chargeback right exists. A chargeback is where the bank who provided the customer with the credit card asks the merchant's bank to refund the money. Chargeback requests can only be made for limited reasons and within limited timeframes. In particular, there may be limitations on chargeback rights where transactions were for gambling or investment purposes.

Remote access scams

What are remote access scams?

Remote access scams are complex scams. They often involve a scammer contacting a customer and gaining access to their computer (or another electronic device) that they can use to transfer funds. Generally, this type of scam involves the scammer calling or emailing the customer pretending to be from the bank or from a telecommunications company, government agency or energy retailer that the customer may use.

Scammers use various complex techniques to access a customer's electronic device. These may include asking the customer to grant them remote access to their device or to download an app that grants the scammer control of the device or can be used to observe keystrokes to obtain passwords. However, the scenario we usually see involves:

- The scammer calls the customer advising the customer has been hacked and they need the customer's help to catch the hackers. Scammers may say the customer's mobile phone or internet access has been hacked.
- The scammer asks the customer to give remote access to their computer or electronic device and asks the customer to log into their internet banking while the hacker has remote access.
- The scammer then makes the screen go blank or puts up a fake screen, so the customer does not see the hacker transferring funds from one of the customer's accounts to another.
- When the screen is removed, the scammer says they have "credited" the customer's account with "baited" funds to catch the hacker. The customer is led to believe these funds were placed there by the caller and may not realise the funds are their own, transferred from another of their accounts.
- The customer then allows the scammer to transfer the funds out of their account to "catch" the hacker.

The crucial difference between remote access scams and investment scams is that the customer usually does not authorise the transfers between their accounts, as the scammer makes them without their knowledge. This means the customer does not realise they are spending their own funds, when they authorise the subsequent transfers to the scammer.

How AFCA approaches remote access scam complaints

AFCA first considers whether the customer authorised the transactions. While each investigation turns on its own facts, we generally take a 'substance over form' approach.

If a customer does not know about or consent to transfers from their accounts to another account, then we consider the customer has not authorised the transfers. If we find the transactions were not authorised by the customer, then we consider whether the customer or the financial firm is liable for the transactions.

Liability for unauthorised transactions is determined by the Code. AFCA will consider whether the customer or the bank should be held liable for the unauthorised transactions under the relevant provisions of the Code. For example, the Code requires us to consider whether the customer contributed to their loss by breaching the passcode security requirements in the Code (such as by voluntarily telling the scammer their internet banking password or providing an SMS code) or unreasonably delaying notifying the financial firm about the transactions. However, liability for unauthorised transactions under the Code is not determined based solely on 'fault'.

To apply the provisions of the Code, AFCA needs to consider all reasonable explanations about how a transaction occurred. We ask the parties to provide us with as much information as possible. Usually we will not know exactly what happened and we will need to decide what is most likely to have happened based on the available information. We will then decide how liability should be apportioned in accordance with all relevant terms of the Code.

Case studies

The following case studies reflect recent AFCA decisions dealing with scams and provide examples of how we apply our approach in practice:

Case study one

The complainant authorised ten separate transactions to an overseas online currency account. The online account was then used to purchase almost $80,000 of online investments which were a scam. To authorise the transactions, the complainant had two phone calls with the bank where she:

- activated the telegraphic transfer service on her accounts to send funds overseas
- increased the daily transfer limit from $5,000 to $50,000.

This complaint considered if the financial firm met its obligation to exercise the care and skill of a diligent and prudent banker and not turn a blind eye to known facts if it knew (or reasonably ought to have known) the complainant was dealing with a scammer.

The complainant first called the financial firm to activate the telegraphic transfer service. The financial firm asked if she was still a student. The complainant confirmed she was no longer a student and now worked in a book store. They asked the complainant who she was sending funds to and whether she knew the recipient. During that call, AFCA found the bank had met its obligations and made reasonable enquiries with the complainant.

Almost four weeks later, the complainant again called the financial firm to increase the daily limit. The financial firm again asked if she was still a student and the complainant gave the same response. The complainant told the financial firm she wanted it increased to purchase bitcoin. The financial firm was initially uncomfortable with the request but did not question the complainant further about the purpose and increased the limit. The complainant then authorised $80,000 of transactions to the online currency account.

AFCA found the financial firm should have reasonably been aware there was a real possibility of the complainant being scammed during the second call because she had not been working for long and was increasing the transfer limit to buy bitcoin. The financial firm did not question the complainant further or warn of the high risk of online currency trading and the prevalence of scams in the geographical location of the merchant.

From the information provided, AFCA found that if the financial firm had the appropriate conversation with the complainant, it would not be liable if the complainant chose to go ahead with the transfers. An appropriate discussion about the reasons behind the complainant's request may have made the complainant think twice before going ahead with the transfers and she may not have suffered further loss.

The financial firm was required to reimburse the complainant almost $80,000 being the disputed transactions she made after the second call, when the financial firm should have been aware of the real or serious possibility of fraud.

Case study two

The complainant authorised transfers of over $400,000 to several overseas entities associated with online binary options traders, who were likely scammers.

This complaint considered whether the bank had any special knowledge that the traders were in fact scammers. If it did, then the financial firm may have had special knowledge of what was occurring or been alerted to a real possibility of fraud and should have taken steps to block the transfers and contact the complainant.

AFCA found the bank had no special knowledge and was not on notice of the real possibility of the complainant being defrauded because:

- the complainant authorised the transactions and did not inform the bank the transfers were to online binary options traders
- the complainant did not ask the bank about the inherent risks with online binary options trading
- the traders' names and details were not listed in any warning notice ASIC sent to the financial firm before the complainant made any of the transfers
- transactions were made by the complainant using the internet banking service provided by the financial firm
- the financial firm had no obligation to monitor the complainant's online banking activities.

AFCA found the financial firm acted appropriately by following the complainant's instructions. It was not on notice of a real possibility of the complainant being defrauded and was not obliged to block the transactions or make further enquiries with the complainant. Accordingly, the financial firm was not required to refund the transfers to the complainant.

Case study three

The complainant was the victim of a remote access scam when scammers tricked her into accessing her computer remotely by calling her and claiming to be from her energy provider. The scammers said the computer was infected with a virus and asked the complainant to download a program which she did. The scammers then accessed her internet banking and successfully withdrew almost $60,000 over multiple transactions.

AFCA found the complainant did not authorise the transactions because she did not knowingly make the transactions or ask the scammer to carry them out. However, the financial firm said the complainant was liable for the disputed transactions because she must have disclosed her passcodes to the scammers, allowing access to her internet banking.

AFCA considered all the information provided by the parties, including a report showing the complainant's computer had been remotely accessed. Weighing the information, AFCA found the most likely explanation was that the complainant logged into her internet banking while the scammer had remote access to her computer. However, there was no information to suggest the complainant was aware the scammers could see the passcode as it would have appeared as a row of dots when she entered it. Therefore, AFCA found the financial firm had not shown she voluntarily disclosed her passcode in breach of the passcode security requirements of the Code.

AFCA also found the complainant likely voluntarily disclosed a second factor authentication code to the scammers. However, under the Code if more than one passcode is required to make a transaction the financial firm needs to prove that the disclosure of the one code contributed over 50% to the customer's loss. AFCA found

the financial firm had not proved this because the financial firm had proved the customer voluntarily disclosed one code, but not the other. Therefore, the financial firm was liable for the unauthorised transfers to the scammer under the Code.

While the financial firm may not have done anything wrong, the Code does not require any fault on the financial firm's part for it to be held liable for unauthorised transactions. The financial firm was required to compensate the complainant for the unauthorised transfers.

Case study four

The complainant purchased a motor car from a legitimate car dealer and successfully authorised the first deposit to the dealer. The complainant was then required to pay a second deposit of almost $40,000. Unfortunately, a fraudster intercepted the details of the second invoice and changed the account details to that of the fraudster's account (the account name was not changed from that of the car dealer). The complainant did not realise the invoice had been hacked and account details changed.

The complainant then mistakenly authorised a $40,000 payment to the fraudster who was an unintended recipient. The complainant thought he was paying the car dealer. The payment falls within the definition of a MIP under the Code because the account name did not match the BSB and account number, since the account the payment was sent to was not held in the car dealer's name.

The complainant notified his financial firm of the MIP after the car dealer did not receive the funds.

In this transaction, the complainant's financial firm acted as the sending bank and the fraudster's financial firm acted as the receiving bank. When a MIP is raised by a customer, the Code places obligations on both the sending and receiving financial firms to promptly attempt to recall the mistaken payment.

AFCA considered the actions of the sending and receiving financial firms and found the obligations set out in the Code had been met. We formed this view because the:

- sending bank warned the complainant that account names are not checked against BSB and account numbers
- sending bank promptly acted on the complainant's request when he notified it of the MIP by sending a recall request to the receiving bank on the same day
- recipient bank responded within five days advising the fraudster had removed funds from the account leaving a balance of $2 before the MIP was raised.

Unfortunately, the funds were no longer available. However, the complainant's financial firm was not required to compensate the complainant for the mistaken payment because all obligations of the Code had been met. Note that the car dealer as the intended recipient of the MIP, could have lodged a complaint against the

receiving financial firm. We would then have considered if the receiving financial firm met its obligations to the car dealer as the intended recipient.

Do you need more information?

This document gives a brief overview of our approach to certain types of scams.

If you suspect you have fallen victim to a scam, please contact your financial firm immediately. You can also visit the **Scamwatch website** for further information on where to get help. If you are unable to resolve your concerns directly with your financial firm, please visit the **AFCA website** about other options available to you, including lodging a complaint with AFCA.

For more information about our complaints process or to access factsheets or approach documents, please visit our **Publications** page.

You can also search our **Published decisions** page. Most decisions about complaints involving scams are classified under the issue type of 'Transactions' and full text searching by keywords (such as 'scam') is also available.

11 March 2021

[redacted]
[redacted]
Australian Financial Complaints Authority

Via email: [redacted]

Dear [redacted]

AFCA fact sheet on scams – consultation draft

Thank you for the opportunity for COBA to comment on this draft fact sheet. I also attach detailed feedback from two individual COBA members.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Customer owned banking institutions account for around three quarters of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition, choice and market leading levels of customer satisfaction in the retail banking market.

COBA members are witnessing an increase in the number and sophistication of scams targeting their customers. The increasing risks to consumers and AFCA's handling of complaints that relate to scams are significant concerns to COBA members.

COBA members welcome action by AFCA to provide information and guidance about scams and AFCA's approach to scams.

However, COBA members have significant concerns about some of the content of the draft fact sheet and about the targeting and intended distribution of the content.

Key points

- **Information and guidance about scams for the two key stakeholder groups, i.e customers and AFCA members, should be appropriately tailored and targeted.**
- **COBA members have identified a range of legal, practical and operational issues arising from material in the draft fact sheet.**
- **COBA requests AFCA to delay publication of this fact sheet, fact sheets or guidance pending further engagement between AFCA and COBA members.**

Targeting factsheets & guidance for different stakeholder groups

We note that stated purpose of the document is:

> "to inform the Australian community about:
>
> - The sort of complaints about scams AFCA commonly sees
> - How AFCA approaches complaints about different types of scams."

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

By targeting the document at “the Australian community”, AFCA may miss the opportunity to communicate effectively with the two key stakeholders: customers and AFCA members (e.g. COBA members).

A fact sheet for consumers should be as simple and clear as possible about how consumers can reduce their risk of being scammed and what to do if they believe they have been scammed.

A fact sheet for an AFCA member should provide useful guidance about how AFCA will interpret legal obligations, legislation, codes and other consumer protection frameworks. This should assist the AFCA member to design, implement and monitor policies and procedures to manage risk and meet required standards.

The 12-page draft fact sheet appears to be an attempt to perform both these quite distinct functions. For example, is the use of case studies intended to assist consumers or AFCA members?

Scrambling messages for the two different stakeholder groups into one document reduces the likelihood of the document helping either group.

In our view, there should be separate documents, appropriately tailored, targeted and distributed.

Clearly outlining responsibilities & obligations

COBA members are concerned there is insufficient information and weight given to customer responsibilities & obligations. COBA members believe a fact sheet would offer more value to consumers if information were provided on how they can minimise their risk of being scammed and clarify that their activities are a consideration in AFCA’s adjudication of these cases.

Members have expressed concerns that the fact sheet implies that financial firms are likely to be required to compensate (in part or full) customers who fall victim to scams regardless of the circumstances or what steps the institution took.

It would be useful to include a clear list of responsibilities and obligations for both customers and financial institutions.

In this regard, it is critically important that consumers have a clear understanding about the need to protect their passcodes.

COBA members have noted a recent pattern of AFCA cases applying a 50-50 ruling to the customer and institution in situations where the passcode was disclosed. Such disclosure is typically a breach of the terms and conditions of the contract between the institution and the customer. COBA members are concerned about moral hazard and sending signals that may encourage risky behaviour.

For example, a COBA member says that “AFCA’s application of the liability provisions in these cases hold financial institutions unjustly responsible for the poor choices made by consumers. With fraud becoming more prevalent, onus should be placed on customers also to ensure they keep their financial information secure.”

Information for consumers should be clear about the distinctions between:

- transactions that are authorised by the consumer but are scams
- transactions that are authorised by the consumer but the consumer now regrets
- transactions that were not authorised by the consumer or are the result of the consumer disclosing their code, and
- mistaken internet payments and scams.

Addressing legal, practical & operational issues

COBA members have identified a range of legal, practical and operational issues arising from material in the draft fact sheet.

The reference to 'diligent and prudent banker' replicates other regulatory standards and may not be an appropriate phrase in the context of scams given it has a specific meaning enshrined in legislation and regulatory guidance.

Members expressed concern that transaction delays due to an institution making reasonable enquiries to ensure the transaction is legitimate may expose the institution to damages or complaints if the transaction was time sensitive. There is no assurance given by AFCA that the institution:

- would not receive a negative determination as a result of a complaint lodged due to delayed transactions while the institution was enquiring about the veracity of a transaction, or
- would not receive a negative determination even if it 'made reasonable enquiries' and received assurances from the customer that a transaction was legitimate (in the event it turned out to be fraudulent).

A COBA member highlighted a section of the draft fact sheet stating: "While the financial firm may not have done anything wrong … the financial firm was required to compensate the complainant." The COBA member questions the value of such guidance if it doesn't offer a solution or suggestion of how financial firms might alter their conduct or their policies.

> "If the draft guidance is considered from a viewpoint of how financial firms may alter their conduct to plan for and prevent poor outcomes, the draft guidance seems of little value because:
>
> - the draft guidance indicates that financial institutions are unable to effectively protect themselves, and
> - no clear guidance on conduct has been provided.
>
> "The logical outcome is that financial institutions profile customers and turn customers away or terminate their relationships if that customer poses a risk of being scammed. Profiling of customers and denial of services is a poor consumer outcome."

Another COBA member has highlighted issues with the "warning signs", such as "spending habits", identified in the fact sheet.

> "In the great majority of cases, it is unrealistic to expect bank staff to undertake an analysis of a customer's spending habits, such that those staff are in a position to identify activity that is out of the ordinary.
>
> "Formal written complaints have been received from elderly customers objecting to invasive questions about transactions such as gym membership payments or streaming service subscriptions. Such complaints are perfectly understandable, and illustrate the difficulty faced by bank staff required to make value judgments about how a customer should or should not be spending their money."

COBA acknowledges that if an institution is aware that a customer has a vulnerability, then it has an additional duty of care towards that customer. However, COBA members believe that the fact sheet conflates the issue of scams and vulnerable customers. COBA members agree that there are actions that institutions can reasonably take to proactively protect customers from scams, such as giving customers warnings about the prevalence of scams. However, unless there is an identified, specific reason, the suggested inquiries are potentially unreasonably intrusive, discriminatory or infringing on a customer's agency to transact on their account.

Even with a vulnerability, it is difficult to see on what grounds an institution could legally deny an otherwise competent adult to access their funds.

Further engagement

Thank you for the opportunity to provide this feedback.

Given the issues and concerns noted above, COBA asks AFCA to delay publication of the fact sheet, fact sheets or guidance pending further engagement between AFCA and COBA members.

Please do not hesitate to contact [redacted] or [redacted] [redacted]) to discuss any aspect of this letter.

Yours sincerely,

MICHAEL LAWRENCE
Chief Executive Officer

Heritage Bank
People first.

Chief Executive Officer
400 Ruthven Street
PO Box 190
Toowoomba Qld 4350
07 4694 9607
lock.p@her tage.com.au

9 March 2021

Mr David Locke
Chief Executive Officer and Chief Ombudsman and
Australian Financial Complaints Authority Limited
GPO Box 3
MELBOURNE VIC 3001

Dear Mr Locke

AFCA's approach to authorised payment fraud

Heritage Bank recognises the important role it has to play in warning and protecting its customers about and against scam activity.

Where the fraud involves a customer willingly making a payment, fulfilling this role comes with particular challenges.

AFCA's current position (as conveyed in recent AFCA determinations involving Heritage) as to the steps Heritage should take to prevent loss to customers who attend a branch to make a payment willingly, but as a result of a fraudulently induced belief, is unworkable.

It is unworkable because it:

1. puts Heritage at risk of breaching State and Commonwealth anti-discrimination laws;

2. puts Heritage at risk of breaching the Privacy Act; and

3. is inconsistent with community expectations.

AFCA's approach to authorised payment fraud

AFCA has recently released for comment a draft *Factsheet – Scams* which is reflective of the approach AFCA takes to the resolution of disputes arising as a result of authorised payment fraud.

AFCA's approach to in-branch authorised payment fraud, as articulated in the draft Factsheet and in its recent determinations, is that the Bank should **identify any warning signs** that the customer might be being scammed, and if those warning signs are present, **make further enquiries** and **document the results** of those enquiries.

Identifying warning signs

AFCA has suggested that warning signs of fraud include:

1. transactions outside the customer's usual spending habits;

2. any apparent vulnerabilities such as age, known or readily apparent medical condition or disability;

3. transactions that are being sent to countries well known to be used by scammers; and

4. customers being secretive or guarded about the purpose of the transfers.

Spending habits as a warning sign

In the great majority of cases, it is unrealistic to expect bank staff to undertake an analysis of a customer's spending habits, such that those staff are in a position to identify activity that is out of the ordinary.

Heritage's experience to date in implementing AFCA's recommendations reflects this. Formal written complaints have been received from elderly customers objecting to invasive questions about transactions such as gym membership payments or streaming service subscriptions. Such complaints are perfectly understandable, and illustrate the difficulty faced by bank staff required to make value judgments about how a customer should or should not be spending their money.

Age as a warning sign

The ACCC's most recent report on scam activity in Australia[1] demonstrates that age is an unreliable indicator of susceptibility to scam activity. The ACCC Report specifically notes as a "Scam Myth" that "*Only older people fall for scams*" observing that people aged 24 to 35 years old send money more frequently than other age groups; people aged 55 to 64 lost the most money to scams, followed by those aged 45 to 54.[2] Very few in those age brackets would consider themselves vulnerable to scams because of their age.

Different treatment in the provision of banking services on the basis of age is prohibited by State and Commonwealth anti-discrimination laws.[3] Adopting age as a factor that triggers the need to ask detailed questions about a transaction (and refusing to process it in the absence of a satisfactory response) risks breaching those laws.

An honest answer given to an elderly customer asking, "Why am I being asked these questions about this payment" would invite complaint to the Human Rights Commission.

Transactions to particular countries as a warning sign

The ACCC Report makes no mention of countries which are well known to be used by scammers.

The ACCC report did refer to the increased prevalence of scams targeting Mandarin-speaking people in Australia, and Australians of Sri Lankan origin.[4] Probing a customer about a transaction and recording their responses because they are Chinese and wish to make a substantial payment to China may be

---

[1] *Targeting Scams 2019: A review of scam activity since 2009* (https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf) ("the **ACCC Report**").
[2] Part 6.1 of the ACCC Report.
[3] Sections 5 and 28 of the *Age Discrimination Act 2004* (Cth). Substantially identical provisions appear in each State's anti-discrimination legislation.
[4] Part 4.6 of the ACCC Report.

unlawful,[5] and On initial reading, this approach seems difficult to disputee. Serious problems arise, however, when it is put into practice in the manner AFCA suggests puts Heritage's staff in an invidious position if asked why different treatment is warranted.

Being secretive or guarded about a transaction as a warning sign

There are many reasons a customer might be guarded about a transaction. Some examples are discussed below. A customer's reluctance to be interrogated about a transaction may be for no other reason than a wish to exercise the right not to have their privacy or correspondence arbitrarily interfered with.[6]

Making further enquiries

AFCA has, via the draft Factsheet and its recent determinations, suggested that where warning signs are identified, Heritage ought to make appropriate enquires, such as:

1. why the customer is sending the money and who they are sending it to;
2. how the customer knows the recipient;
3. whether the customer has met the recipient, dealt with them before or researched their legitimacy;
4. whether the customer has discussed the transfer with a family member, friend or trusted advisor;
5. asking for a copy of a document showing the purpose of a transaction; and
6. in the case of a joint account and in the absence of a satisfactory explanation for the transaction, telephoning the other joint account holder.

A customer wishing to make an unusual yet perfectly legitimate and authorised payment is likely to be affronted by these enquiries, however well-intentioned they are.

A customer sending money to an intimate partner overseas who he or she happened to meet over the internet is likely to take Heritage's questioning and warnings about the prevalence of romance scams very poorly. A customer transferring money for immoral but nevertheless perfectly legal purposes will naturally be guarded about the reasons for the transfer, and will be perturbed by detailed questioning and note-taking about its purpose.

It is conceivable that the difficulties with the approach to further enquiries suggested by AFCA will not be limited to customer relations.

A victim of intimate partner violence who wishes to transfer funds out of a joint account might understandably be guarded about the reasons for the transaction. Reluctance to proffer a fulsome explanation might be due to embarrassment about the situation, the effects of their partner's ongoing coercion and control, or fear of the consequences if the payment is discovered. Further interrogation about such a transaction will be distressing. A telephone call to the joint account holder could be catastrophic.

These are very difficult decisions for Heritage's front-line staff to make about many thousands of transactions that take place every week.

Documenting the Bank's enquiries

---

[5] See sections 4 and 13 of the *Racial Discrimination Act 1975* (Cth) and the equivalent State anti-discrimination legislation.

[6] See section 25 of the *Human Rights Act 2019* (Qld). Equivalent legislation has been enacted in other States.

AFCA has recommended Heritage keep detailed records of its questions and customers' responses.

The vast majority of transactions in which warning signs are present will be legitimate. Following AFCA's approach, Heritage will collect and retain a considerable volume of detailed personal and sensitive information about legitimate transactions.

Heritage is bound by the Australian Privacy Principles. Australian Privacy Principle 3 ("**APP 3**") concerns the collection of solicited personal information. Under APP3, a bank may only collect personal information which is reasonably necessary for one or more of the entity's functions or activities. APP3 also protects the collection of sensitive information, which includes information concerning an individual's political associates, memberships of professional or trade associations, sexual preferences or ethnic origins. It is foreseeable that answers to the questions AFCA suggests be asked and recorded will contain sensitive information. Such information may be collected only when (relevantly) authorised by law, or where a "permitted general situation" exists.

As set out below, Australian law does not oblige Heritage to query transactions, give warnings about fraud or collect information about its customers' transactions.

Permitted general situations include preventing suspected unlawful activity. It is doubtful that the existence of the warning signs identified by AFCA is capable of giving rise to the level of suspicion necessary to protect the Bank from breaching APP3.

Heritage is regularly compelled by Family Court subpoenas drafted in wide terms, capable of requiring disclosure of information such as that collected in connection with transactions flagged as suspicious (applying AFCA criteria). This is one example of the circumstances in which the confidentiality of sensitive information collected in relation to legitimate transactions may be compromised.

The management and protection of a considerable volume of personal and sensitive data generated as a result of AFCA's approach imposes a heavy burden on Heritage.

The legal position

Heritage accepts that the legal position regarding authorised payments is not determinative. It is, however, relevant to the extent that the Bank's legal obligations are matters AFCA is required to have regard to in determining disputes. It is relevant also to community expectations, as the community would expect AFCA's approach to resemble the legal position in some way.

The legal position in Australia is broadly consistent with the United Kingdom. The very recent consideration of a bank's duties in relation to authorised payment fraud in the United Kingdom[7] enables the legal position to be stated shortly and authoritatively as follows:

1. there is no legally recognised duty on the part of the bank to protect its customer from payments willingly made in reliance upon a fraudulently induced belief, for reasons including that such a duty conflicted with the established duty on the part of the bank to comply with its customer's mandate;

2. the bank is under no duty to have in place policies and procedures directed to avoiding loss arising from authorised payment fraud;

[7] *Philipp v Barclays Bank UK Plc* [2021] EWHC 10 (Comm) ("***Philipp***") (https://www.bailii.org/ew/cases/EWHC/Comm/2021/10.pdf).

3. there is no duty on the bank to ask any safeguarding questions of customers; and

4. by reason of the absence of any duty on the bank to prevent authorised transactions, the bank cannot be liable for loss caused as a result of an authorised payment.

The absence of any legal duty on the part of banks to query transactions or issue warnings has been accepted by the United Kingdom Financial Ombudsman Service since 2015.[8] The manner in which those duties is articulated in *Philipp* therefore comes as no surprise.

Community expectations

Heritage must also consider the expectations of customers wishing to perform legitimate transactions with their own money promptly and free from interrogation. It must be alive to the possibility that those customers consider that they are perfectly capable of safeguarding their own interests, and qualifying their right to deal with their funds as they see fit is too great a price to pay for protection from the potential for loss as a result of fraud.

The community understands that the freedom we value in Australia has as its corollary an obligation to take personal responsibility for mistakes made. There is no question that Australians expect financial institutions to treat people fairly, but the community does not expect its financial institutions (in which many have an interest) to act as insurers of last resort for victims of fraud.

A code for authorised payment fraud

Second-guessing a customer's instructions requires the bank to tread a very fine line. It requires balancing the desire to, where possible:

1. protect the Bank's customers from loss caused by scam activity; and

2. recognise and protect the rights and freedoms of those customers who wish to undertake a legitimate transaction that might share some of the (constantly evolving) characteristics of a fraudulent transaction.

As observed in *Philipp*, second-guessing a customer's own outwardly genuine instruction by raising safeguarding questions should be supported by a clearly recognised banking code defining the circumstances in which the need for such questions would be triggered, and the circumstances in which banks should not act (or act immediately) upon its customers' genuine instructions. If banks are to be held to the standards of something equivalent to a code for intervention, then they need to know its terms and be able to apply them.[9]

Heritage is of the view that such a code for intervention would also promote consistency in the approach of Australian banks to the issue.

It is vital that the approach of Australian banks and financial institutions to the complex issue of authorised payment fraud be supported by the certainty of workable standards of action through an industry code, developed through careful consideration of the competing legal obligations, community expectations and in consultation with industry stakeholders.

---

[8] Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015 (https://www.financial-ombudsman.org.uk/files/1763/vishing-insight-report2015.pdf) pp. 6 and 26.

[9] *Philipp* at paras. 159-161.

Heritage would welcome the opportunity to participate in further discussions regarding AFCA's position on authorised payment fraud and the potential development of an industry code to address the issues raised in this letter.

Yours faithfully,

Peter Lock
Chief Executive Officer

Benn Wogan
General Counsel and Company Secretary

AFCA Factsheet – Scams
Submissions

AFCA released the (draft) Factsheet – Scams on 23 February 2021. COBA have called for points for a submission on issues raised by that draft factsheet.

1. Value of factsheets

1.1. Factsheets prepared by regulators are typically an invaluable source of guidance. Factsheets help financial institutions to:

(a) Understand how a regulator interprets legal obligations and intends to apply the law;

(b) Assess processes already in place against recommended processes as described in the Factsheets; and

(c) Adjust policies and procedures is necessary to achieve the desired risk weighted outcome appropriate for the circumstances.

1.2. Often, the case studies provided in factsheets also provide a very practical and tangible understanding of how the legal obligations should be applied to specific examples.

1.3. There are some examples of expected conduct, for example:

> *"…all financial firms should display an onscreen warning when a customer authorises an electronic transfer …"*

1.4. However, the guidance then goes on to infer that there appears to be no possible conduct a financial firm could adopt to protect itself from certain adverse outcomes. Specifically,

> *"While the financial firm may not have done anything wrong … the financial firm was required to compensate the complainant …"*

1.5. Query where the value in this guidance is then if it doesn't offer a solution or suggestion of how financial firms might alter their conduct or their policies.

2. Conduct of financial firms

2.1. The guidance indicates that financial firms should take an active role in customer education about scams. However, that role ought naturally sit with government agencies, because to encourage customers to feel safe taking advice from financial firms seems counter intuitive to education that is effectively educating customers not to take financial action from people holding themselves out to be a financial advisor or similar.

2.2. The trust building that comes through education should be built with Government agencies that customers are able to trust rather than the private sector.

2.3. There appears to be no conduct a financial firm can take to prevent itself from exposure to scam claims and payments.

2.4. If a customer is caught up in most types of scams, then the AFCA appears to be to require the financial firm to compensate the customer for that scam.

3. Customer outcome

3.1. If the draft guidance is considered from a viewpoint of how financial firms may alter their conduct to plan for and prevent poor outcomes, the draft guidance seems of little value because:

(a) The draft guidance indicates that financial institutions are unable to effectively protect themselves; and

(b) No clear guidance on conduct has been provided.

3.2. The logical outcome is that financial institutions profile customers and turn customers away or terminate their relationships if that customer poses a risk of being scammed.

3.3. Profiling of customers and denial of services is a poor consumer outcome.

3.4. There have been similar submissions by foreign aid organisations in relation to AML restrictions whereby the foreign aid organisations have reduced access to financial services and reduced charitable payments being made because the restrictions being imposed by financial firms on the international transfer of funds is being so tightly restricted. That is a poor customer outcome too, and this is similar.

4. Alternatives

4.1. Where a financial firm cannot budget for such likely expenditure due to its unknown quantum and occurrence, and where Government agencies are best placed to educate customers in relation to financial crimes and scams, then perhaps an externally administered fund would be best placed to administer compensation payments.

4.2. An external scheme could be funded by industry levies, however the separation of functions – with a move away from the private sector – would also support customer education.

4.3. Customers may still receive the similar compensation amounts, but through a different – and arguably more appropriate – channel.

4.4. Payment of levies as opposed to ad hoc compensation would also allow financial firms to budget and project costs and expenditure.

4.5. The use of industry wide levies and external schemes would also assist to level the playing field and reduce an ever increasing divide between big banks and smaller players. At the moment, that divide is increasing as big banks may afford to make large settlements rather than disputing those claims.

4.6. If it indeed is an appropriate policy initiative to compensate customers who have fallen victim to scams, and if this is an industry wide issue, then perhaps an external and independent fund can be established, perhaps funded by industry levies, where that fund can then pay out affected customers.

4.7. Such an independent and industry wide arrangement would create a level playing field between financial institutions, whereby the larger financial institutions would not contain a competitive advantage over the smaller financial institutions on account of having deeper pockets, or not.

5. Financial implications

5.1. On the basis that there is no apparent way of a financial firm protecting itself from claims of scams (for example there is not a system upgrade, or change of procedures, or additional staff training that could reduce the risk), there is also no way for financial firms to predict the future cost of having to compensate customers who have fallen victim to scams.

5.2. For example, there can be no presumed percentage allocated for the costs of claims, making it very hard to budget for.

5.3. In addition, for customer owned banking associations without shareholders, any costs that are allocated to pay for scams as described in the guidance are effectively paid for by customers.

5.4. Accordingly, the question arises, ought an allocation for the cost of scams be an insurance cost and choice that consumers themselves make?

5.5. Might the money be better spent on consumer education or more intelligent systems for the financial institutions?

5.6. The Factsheet has not clarified when a financial firm would be liable and ought therefore pay out the claim, or when it is reasonable for the financial firm to progress the matter

through AFCA. However, financial firms incur a case cost for each case that is taken through the various AFCA processes.

6. Timing

6.1. There is no guidance as to the length of time in which AFCA will respond to a scam complainant. As an example one AFCA matter (which is remarkably similar to case study three) was submitted for a Determination in October 2020 and as at 3 March 2020 we still have no response and have not been kept up to date or informed of internal service levels.

AFCA Factsheet – Scams Submissions

	AFCA Factsheet – Scams: Quotes	Comment
1	Usually, because of the deception involved in these scams, the customer authorised the transactions (i.e. made them themselves and intended to do so) but did not realise they were paying a scammer. - Page 2	Ergo the e-payments code should not apply because the transactions were 'authorised'. Fundamental difference here in how 'authorisation' has been interpreted. It should be interpreted in light of a deception.
2	Financial firms do not have a genera l obligation or duty of care to observe or monitor their customers' transactions, or to maintain watching briefs of scams for its customers' benefit. - Page 3	Financial firms are firms with commercial interests and should be able to pursue those interests and not spend money maintaining systems to try and deal with emotional vulnerabilities played upon by scammers.
3	At law, a financial firm has a duty to act as a prudent and diligent banker. - Page 3	Where? What is the extent of that duty? Not referenced in the fact sheet.
4	A financial firm cannot turn a 'blind eye' to warning signs that indicate their customer may be at a real risk of being scammed. - Page 3	No guidance as what those warning signs might be or what to do about them, other than flagging, and monitoring known scams and closing down those avenues. Cannot predict a scam.
5	AFCA will consider: (1) if ASIC issued a warning notice to the financial firm about the recipient of the funds before the customer sent the funds; (2) where a transfer is in branch there may be a heightened expectation; and (3) if Fraud has flagged the transaction as suspicious then the financial firm may be on notice.	What about customers explanation if a transaction is marked as suspicious? Is the financial firm off the hook if they asked the question and then unflagged the transaction?

6	Warnings signs may include: (a) Transactions that are outside the customer's usual pending habits; (b) Transactions that are being sent to countries well know to be used by scammers; (c) Any apparent vulnerabilities such as age or medical disability; and (d) The behaviour of the customer when speaking with the financial firm such as being secretive or guarded or talking to another person on the phone while giving instructions to the financial firm.	'May' include means this is not an exhaustive list.
7	Where a bank identifies a warning sign it should make meaningful enquiries with the customer to see if they are being scammed.	No advice of what to do once those enquiries have been made.
8	If the customer still appears confused or is unable to reasonably show that the transaction is legitimate, it may be appropriate for the financial firm to refuse to process the transaction until it can be satisfied that the transaction is legitimate.	Will banks be opened to damages from transaction delays? Eg if a payment needs to be made on a particular day and there are perhaps penalties if not paid that day but the transaction gets delayed - then what?
9	If a financial firm does not meet its obligations to act as a diligent and prudent banker, it may be required to compensate its customer for all or part of their loss.	Does this refer only to AFCA enforcing that compensation?

10	[Invoice hacking scams] will usually will the definition of a mistaken internet payments (MIP) under the ePayment Code (Code).	Ok, because there is guidance on conduct. Eg Financial firms must (under the Code) display an onscreen warning when a customer authorises an electronic transfer advising that: - the financial firm does not check the account name matches the account number or BSB of the payee account; - the funds may be unable to be recovered if they are paid to the wrong account.
11	Case Study One: The financial firm did not question the complainant further or warn of the high risk of online currency trading and the prevalence of scams in the geographical location of the merchant.	Warning of the risk of a particular type of financial investment is a provision of financial advice, which ADIs are generally prevented by law from doing (as licensing restrictions generally prevent ADIs from providing financial advice). AFCA should not require ADIs to do something that is not generally legal.

12	Case Study Three: Under the Coe if more than one passcode is required to make a transaction the financial firm needs to prove that the disclosure of the one code contributed over 50% of the customer's loss.	(1) The definition of 'authorisation' in this context is at issue and is not consistent with a financial firms definition of 'authorisation' under the terms and conditions of an account – AFCA should clearly explain that specific T&Cs have no value or effect if AFCA do not think they do; and (2) The case study example and sentence of how the Code operates is both confusing and incorrect – it is not 50%, it is either 100% or 0%. It is also not AFCA's role to interpret the Code. What is the point of two factor authorisation if it does not protect a financial institution? Should there be three factor authentication to overcome this 50% hurdle, but that would be very restrictive for customers to spend their own money?
13	While the financial firm may not have done anything wrong … the financial firm was required to compensate for the complainant for unauthorised transactions.	If there is no conduct the financial firm could have taken to protect itself then where is the value in the guidance?