Australian Banking Association

ABA response to AFCA scam fact sheet

ABA welcomes the opportunity to provide input to AFCA's draft scam fact sheet.

Scams is a priority for the ABA in 2021 and in the coming period. ABA is working with AusPayNet on industry wide initiatives and would be pleased to discuss our initiatives further with AFCA. ABA and AusPayNet are also engaged in ASIC's proposed consultation on the ePayments Code. As AFCA would be aware, scams are evolving including in response to current events. Scammers have sophisticated methods to groom/coach potential victims, and it can be challenging for bank staff to question a customer who has fallen victim to a scam. If a bank asks questions or decides to stop a payment, the customer can take their account to another bank and try again.

Our comments and questions about the draft scam fact sheet are made in this context. However the ABA is raising material concerns about the intent and content of the factsheet and seeks discussions with AFCA prior to the factsheet being finalised.

General comments

Guidance and further discussion between AFCA and industry

In a number of areas, ABA is seeking further discussions with AFCA with the aim of obtaining more specific industry guidance from AFCA. Examples of areas where we are seeking such guidance include what may constitute a warning flag about age and how banks should act in particular circumstances and when banks should consider stopping a payment.

Guidance from AFCA can ensure greater consistency in banks' responses to scams. This can provide a more positive experience for customers, particularly if there is greater clarity and consistency between the sending and receiving banks about what actions will be taken. This might also reduce the incentive for scammers or customers to 'forum shop' by moving between banks. The ABA believes guidance can be given in key areas without taking away from AFCA's flexibility to assess complaints on a case by case basis.

The ABA also seeks further discussions with AFCA about the time required to implement some of AFCA's expectations, and interpretation of key provisions in the ePayments Code of unauthorised transactions and the liability provisions.

Purpose and intended audience

ABA considers the purpose of the factsheet needs to be clarified and be more focused. Currently it is not clear whether the factsheet intends to:

- educate consumers about the types of scams they may encounter;
- provide guidance about what consumers can expect from their financial institution in terms of potential reimbursement; or
- provide guidance to industry about AFCA's expectations.

ABA believes the factsheet should focus on content directed at consumers, and content that is directed at industry should be in a separate document. A document for industry has more scope to set aspirational expectations, if it does so with the understanding that it may take some or all institutions time to make changes and meet those expectations. An industry document could also set clearer guidance about when AFCA *may*, depending on the facts of the case, find a bank liable. If the same document is published for consumers, it is likely to raise unrealistic expectations from consumers that they *will* receive a refund, even when the facts in the case mean the consumer would not be eligible or there will be apportionment of liability.

ABA asks AFCA to consider the role of the case studies, and whether they are intended to educate consumers about common types of scams or the methods used by scammers. Given the speed at which scams evolve, the case studies need to be reviewed for currency and may need to be updated regularly. The case studies in the draft factsheet are already dated and do not reflect current methodologies by which customers are targeted. This has the potential to mislead customers or create a false sense of security. Further, if the cases studies are intended to educate consumers about scams, this document may not be the right vehicle as in most cases the customer will already have fallen victim to the scam by the time a matter reaches AFCA.

ABA also asks AFCA to consider what kind of detailed information may *not* be appropriate for a public document, as it can unintentionally aid scammers and complaint management companies. Publishing industry-focused detail, such as what questions AFCA expects banks to ask can assist scammers to coach their victims to avoid a bank's controls. Stating that banks should not turn a blind eye to 'red flags' can be used by complaint management companies to argue that a bank has done so and should refund a customer, even if the facts of the case may not support that conclusion.

Instead, ABA asks AFCA to include information that provides a fuller context for discussions about scams. This includes an explanation of social engineering and how this is used by scammers to manipulate victims, highlighting a consumer has responsibility to protect themselves from scams, and highlighting the risks associated with providing secure codes, messages, tokens, or device access to any other person as this can impact on the security of the account.

In summary, the ABA asks AFCA to consider issuing a shorter public document with a clear purpose and a more holistic explanation about scams, and separately provide industry guidance. If AFCA wishes to engage in further consumer education about scams, the ABA would be very happy to discuss potential vehicles and initiatives with AFCA (and ASIC).

Implementation

A number of banks will need to undertake internal work – potentially significant internal work – to fully address aspects of the factsheet. This work can include providing clear warnings to consumers via digital or front line channels when customers make a first time payment to new payees. As such ABA is opposed to AFCA issuing the factsheet in its current form unless publication is significantly delayed, so industry can undertake implementation work prior to the factsheet goes 'live'. ABA recognises this is not an attractive option.

A preferred alternative would be, as suggested above, issuing a shorter public document that does not set unrealistic expectations for consumers, and at the same time providing industry guidance that recognises the practicalities for industry including time needed for industry to implement some enhancements.

Case studies

While romance and investment scams, business account hacking, and remote access scams are common types of scams, the case studies are already dated as scams evolve rapidly. ABA asks AFCA to consider more recent scam types such as inheritance and ATO scams, and other scam types.

ABA has additional comments about specific case studies:

- In relation to investment trading platforms: many are legitimate, and just because a customer may lose money from their investment does not mean it's a scam. Financial firms are not liable for an investment risk taken by the customer.
- Similarly, it would be problematic if AFCA expects banks to assume that cryptocurrency and binary options related transactions are likely to be scams and query each transaction. A large volume of such transactions are made each day, many to legitimate businesses. Only a very small number may be suspicious.
- For many scam types, if a payment is made online, then authorised online transfers do not provide the bank with an opportunity to stop the transfers and make inquiries of the customer. This should be clarified in any public document and case studies, as well as reflected in AFCA's assessment of the case and should recognise that there is no basis to refund the customer.

Australian Banking Association

Investment and romance scams

ASIC warning notices

Banks are using ASIC 'do not deal with' lists or warning notices in their monitoring for suspicious transactions. However, the usability of data provided by ASIC vary and some data are not provided in a usable form. As such we consider that AFCA's assessment should take into account whether a specific ASIC warning notice included all data that a bank needs to apply in its real time monitoring. For example:

- Recipient accounts are not always reported by the customer and so would not be provided by ASIC.
- If ASIC's warning notice only includes a name, there will be discrepancies between the name reported by the customer and/or the name linked to an account. This can make detection almost impossible.

ABA also notes the frequency of warnings from ASIC has decreased significantly (down to quarterly). This may highlight the difficulty that ASIC is facing in determining whether something is a scam and a warning ought to be issued.

Looking forward, ABA understands that AFCX and ASIC are in dialogue about making ASIC warning notice data more consistent and improving its ease of use for the banks (noting not all banks are members of AFCX). For these reasons we ask AFCA to take into account the quality of data received from ASIC and whether it was in a form that can be used by a bank on a case by case basis.

Warning signs and what banks should do

ABA seeks more specific guidance from AFCA on aspects of warning signs:

- Age as a warning flag of vulnerability: the ABA asks AFCA to be more specific about the minimum age that should be taken as a warning flag. It would not be desirable for banks to apply different age thresholds, and banks are likely to face competition or other legal risks if banks seek to agree on a common approach. Guidance from AFCA would also help banks to explain to consumers why a bank is making additional queries.
- 'Transactions that are being sent to countries well known to be used by scammers' (page 3) is broad. ABA seeks clarification whether this is intended to line up with other AML / CTF watch lists or other financial crime sanctions lists. Further, the majority of transactions sent through remitters are not fraudulent or scams, acting on the basis they are likely to be scams will create significant inconvenience for some customers that rely on these services.
- Further discussions between AFCA and industry would be helpful to clarify the application of AFCA's expectations about certain warning signs.

What banks need to do: ABA seeks further discussions with AFCA about how this expectation may be applied in some scenarios.

- ABA seeks clarification whether AFCA expects banks to treat all payments to first time recipients as suspicious. For example, in some institutions, 1 in 5 payments made by consumers using online banking are to a first time recipient. In addition to the bank's resource constraints, querying each payment to a new recipient would impose significant inconvenience on consumers, undermining the efficiencies and benefits of instant payments achieved by new payment infrastructure (such as NPP).
- Customers may not be receptive to banks making inquiries about proposed payments, particularly if a customer engages in a number of legitimate transactions that may raise 'warning flags' and banks are always expected to ask customers for documents to show the purposes of the transaction. The types of questions that AFCA expects banks to ask can diminish trust between a customer and their bank. ABA asks AFCA to discuss with

banks and issue guidance on, for example, whether it is always appropriate to ask for documents as set out on page 4.

- A bank may issue generalised warnings to customers about scams before a customer makes a payment to a scam, but the generalised warning is not triggered by any 'red flags' about the actual payment. ABA asks AFCA to discuss with banks and give guidance on what may be a customer's obligation to read and act on warnings and when the banks should not be held liable. Without such guidance, this risk can be a disincentive to issue general education and warnings.

Invoice hacking scams

MIP definition

ASIC is proposing to consult on changes to the ePayments Code including the definition of mistaken internet payments. The change are expected to clarify that MIP only applies to 'fat finger' errors and not authorised payments as in invoice hacking scams.

It may be confusing to consumers if AFCA's fact sheet provides case studies based on the existing MIP definition and needs to be amended within a short time.

ABA has also discussed with AFCA that applying a fraud stop process can be more effective than the MIP process. AFCA has informally acknowledged this and suggested banks can explain to AFCA why a bank followed a different process in a given case. However, banks need confidence they can take this action. As such ABA strongly encourages AFCA to provide industry guidance about when it may be appropriate to apply fraud stop rather than MIP, and the documentation that banks should maintain to support such decisions. The ABA would be happy to discuss this request for guidance with AFCA.

If AFCA does provide such industry guidance, it would also need to ensure any consumer facing document does not give a contradictory message.

Banks need to display prominent warnings

ABA and banks strongly encourage AFCA to provide more specific guidance on the types of warnings that it considers to be current good industry practice. The ABA notes this guidance can be updated over time as AFCA observes better practices (with due consideration for the cost and time required to implement changes).

Chargebacks

Depending on the purpose of the document, ABA seeks separate and more detailed guidance about chargeback claims. It is usually the Visa or Mastercard scheme rules that apply, so it would help for AFCA to drill down more into the reason codes and approaches, since customers often expect the chargeback claim to succeed when using their credit card account for transfers. We also ask AFCA to consider if the recall obligations can be explained more simply for consumers.

Remote access scams

Meaning of unauthorised transactions

ABA seeks further discussions with AFCA about the term 'unauthorised transactions' and the allocation of liability. ABA notes ASIC is considering changes to the ePayments Code that may have an impact on these issues, and would welcome the opportunity to discuss with AFCA the questions relating to 'unauthorised transactions' definition and the liability provisions under the ePayments Code.

- ABA would like to discuss with AFCA the meaning of the term 'unauthorised transactions'. There is discrepancy between how this term is used by AFCA and how it is understood by the financial crime detection and banking industries. The factsheet uses this term to refer to transactions that industry would consider to be *authorised but unintended*, rather than *unauthorised*.

- In the example given on page 7, the victim was socially engineered to provide remote access to their computer, likely via a legitimate remote access tool. The customer 'authorised' the final payment to the scammer though the intention was to catch the hacker. ABA believes it can be misleading to refer to this example as 'unauthorised' without further qualification.
- ABA also seeks a discussion with AFCA about when a consumer is taken to have contributed to the loss or contributed to more than 50% of the loss, and the application to case study 3 as well as other issues such as screen scraping. In these cases the customers' actions occur outside of the bank's control, the bank has no role in the authorisation of the transaction and may have no way to detect the breach or red flags. As such the bank is powerless to stop the scam.

These questions relate to ABA's earlier comment that the factsheet should provide more information about the consumer's responsibility to protect their devices and credentials. ABA is particularly concerned about the explanation on page 8, which appears to imply that by sharing their credentials a customer may not be liable for the loss. This sends the wrong message about security, and can set unrealistic expectations for consumers, as they may believe that their bank will always refund them even when they have failed to take steps to protect their device or credentials.

Case studies

The ABA considers case studies 1 and 2 in this section are problematic. Many binary options investments or cryptocurrency transactions may be risky but are not scams. It would be problematic for banks to act on the assumption that many of these are scams and will open banks to criticism of de-banking certain businesses or customers.

In relation to case study 4, ABA asks AFCA to more clearly explain that a recall request on the same day still may not work and clarify when a receiving bank may and may not be liable (noting there has been determinations against a customer where a bank is the receiving bank in a mistaken internet payment).