Reforms to the Payment Systems (Regulation) Act 1998 – Exposure draft legislation

Submission to the Australian Government - Treasury

November 2023

Australian Financial Complaints Authority

Contents

Introduction

The Australian Financial Complaints Authority (**AFCA**) is the independent external dispute resolution (**EDR**) scheme for the financial sector. For over 25 years, AFCA and its predecessor schemes have provided fair, independent, efficient and effective solutions for Australian consumers and small business to have their financial complaints resolved.

In addition to providing solutions for financial complaints, AFCA has responsibilities[1] to identify, resolve and report on systemic issues and to notify the Australian Securities and Investments Commission (ASIC), and other regulators, of serious contraventions of the law. AFCA works closely with ASIC and regularly liaises with it to share complaint insights, to inform and assist its regulatory work.

AFCA's Code Team supports independent committees to monitor compliance with codes of practice in the Australian financial services industry, and to achieve service standards that people can trust.

More broadly, AFCA plays a key role in restoring trust in the financial services sector. Since its establishment on 1 November 2018, AFCA has handled over 367,000 complaints and delivered over $1.07 billion in compensation to consumers. Its systemic issues work has resulted in 4.8 million people receiving more than $340 million.

AFCA welcomes the opportunity to provide a brief submission[2] in response to Treasury's consultation on Reforms to the Payment Systems (Regulation) Act 1998 – Exposure draft legislation.

Observation and Insight

AFCA's role as the EDR scheme for the financial services industry arises out of the licensing obligations in the Corporations Act 2001 (the Act). While these reforms do not directly impact AFCA's membership or operating Rules, an efficient and resilient payments system is critical to consumer confidence and safety in their financial transacting.

AFCA therefore broadly supports the reforms and underlying objectives proposed in the exposure draft legislation, including expanded consumer protections and increased capacity in the regulatory framework to address emerging risks.

[1] Refer to Part C, Reporting Requirements, of ASIC Regulatory Guide 267: Oversight of the Australian Financial Complaints Authority.
[2] This submission has been prepared by the staff of AFCA and does not necessarily represent the views of individual directors of AFCA.

We observe the shifting landscape around how Australians interact with their financial institutions, including that 25% of card transactions in Australia are now made through mobile wallets[3].

The Australian Banking Association and Accenture *Bank on it – customer trends 2023 report*[4] starkly shows the rapidly increasing use of mobile wallets. This includes:

- Over 15.3 million cards were registered to mobile wallets in 2022, up from just over two million cards in 2018 – a 760% increase
- The value of mobile wallet transactions reached $93 billion in 2022, up from $746 million in 2018 – a 12,400% increase
- The number of mobile wallet transactions increased to 2.4 billion from 29.2 million – an 8,200% increase.

As this trend is likely to continue to increase over time, we recognise the importance of updating the definition of payment system 'Participant', to ensure all entities involved in the payments value chain are captured. This includes Buy Now Pay Later (BNPL) facilities and digital wallet services facilitating payments by storing digital representations of payment cards.

Increasing numbers of unauthorised transaction complaints

Since the inception of AFCA in 2018, complaints relating to unauthorised transactions has been the top issue raised by consumers in the Banking and Finance space. Even accounting for this fact, AFCA saw a significant increase in unauthorised transaction complaints in the last financial year from 6,174 (2021/22) to 10,614 (2022/23).

Personal transaction accounts overtook credit cards as the most complained about product in 2022–23, with disputes up 86%. It was the first time credit cards have not topped this list since AFCA's inception. There is likely to be many underlying reasons for the change, including an increase in the take up of various payment methods and in part due to scam related complaints.

Issue	2018-19	2019-20	2020-21	2021-22	2022-23
Unauthorised transactions	2,839	4,915	4,878	6,174	**10,614**

[3] A strategic plan for Australia's Payment System - Building a modern and resilient payments system (pg. 8)
[4] Australian Banking Association (ABA) and Accenture - Bank On It – Customer Trends 2023 report

Scams

In the 2022/23 Financial Year, AFCA received a 46% rise in serious financial crime and scam related complaints, which averaged more than 500 a month - 6,048 for the year. From July 2023 to date, we have seen an even more significant (and concerning) increase in scam related complaints lodged. As a result of the increasing number of scam related complaints being lodged with AFCA, we witness on a daily basis the significant impact this issue causes consumers.

According to the Australian Bureau of Statistics, in 2021-22, two thirds of Australians aged 15 years and over were exposed to a scam[5]. As scams continue to evolve and related complaints increase, AFCA is working closely with industry, regulators and governments to keep our approaches to this dynamic space aligned, and to ensure we help consumers and financial firms resolve complaints efficiently and fairly.

We recognise the Government's significant initiative in setting up the National Anti-Scam Centre and the positive steps that some banks have taken to protect consumers. However, not enough is being done by all banks and there is no consistency in approaches. Consumers continue to bear the bulk of the losses from financial crime, yet the level of sophistication and complexity of scams makes it difficult for people to protect themselves from this activity.

AFCA believes there is a pressing need for strong, uniform protections for consumers, including appropriate settings for payments systems regulation. We look forward to engaging further with Government, industry, and consumers groups on these issues.

Digital Wallet Determination – Case study

The below case study was included in AFCA's 2022/23 Annual Review and provides an example around the complexity of issues faced with these transactions.

Background

The complainant received a text message stating she had an outstanding toll road invoice. She clicked on a link that took her to what she thought was the legitimate toll road operator's website. Then she entered her credit card details to pay the invoice.

The website was fake and was used to harvest the complainant's credit card details and a one-time password (OTP), which the complainant thought was needed to authorise the toll payment. This enabled the scammer to load the credit card as a digital card onto their own mobile phone.

[5] https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams

Shortly after, the scammer used their mobile phone to make 16 transactions of $1,000 each at well-known retail stores. No further PIN or pass code was required to make the disputed transactions. The complainant reported the disputed transactions to her financial firm the following day.

The financial firm said the complainant had authorised the disputed transactions because, by allowing the scammer to add the credit card details to the digital wallet, she must have disclosed the OTP.

Findings and outcome

The ombudsman found the disputed transactions were unauthorised. This meant the liability provisions of the ePayments Code (the Code) applied. Under clause 10.2 of the Code, a card holder is not liable for unauthorised transactions that are made using an 'identifier' without a 'pass code' or a 'device'.

A digital card is an 'identifier' and the disputed transactions did not require a pass code or device. The mobile phone onto which the digital card was loaded was not a device as defined by the Code. Therefore, under clause 10.2 of the Code, the financial firm was liable for the disputed transactions.

The financial firm said the complainant breached the pass code security requirements of the Code, which requires card holders not to disclose pass codes that are needed to perform transactions (clause 12.1). The financial firm said the complainant must have disclosed the OTP to enable the credit card to be added to the digital wallet.

The ombudsman found the complainant did not knowingly disclose the OTP to the third party. She thought she was engaging with a legitimate website to authorise a payment. The OTP was not a pass code needed to 'perform a transaction'. The Code distinguishes between pass codes needed to perform transactions and pass codes needed to authenticate users (which the OTP arguably did). A card holder is only liable if they disclose pass codes needed to perform transactions.