EPA ASIA

ROUND TABLE
THE ROLE OF REGIONAL INDUSTRY COLLABORATION IN COMBATING SCAMS

JULY 2023

It seemed too good to be true…

An industry fireside chat covering payments innovation and scams, generous networking drinks and canapes hosted by EY and organised by the EPAA in stunning surroundings…

But wait, there's more – preceding the networking a session of 20 industry professionals assembled for a 2-hour discussion regarding scams, expertly led by Paul Franklin who, until recently, enabled technology solutions for the CDR at the ACCC.

"It seemed too good to be true. But then there is always that part of you that says, 'What if I am about to miss out on the bargain of the century?"
- smh.com.au, 27.05.2023

Sounds too good to be true? No, it really happened and appeared to be an excellent investment of time for all attendees.

The distinction between payment scams and fraud

Whilst there is overlap, in general, payments fraud is commonly defined as an unauthorised payment made from an account without the permission of the account holder. Payments scams occur when an account holder is tricked into authorising a payment from their own account or sharing information that enables the scammer to authorise a transaction by impersonating the account holder.

A large and growing problem

Recently released figures for scams have led to commentators claiming we are now in a "scamdemic"...

Scammers are well resourced, have access to AI, and likely business plans, budgets and stretch targets!

And, assisted by technology, they are becoming far more sophisticated. Gone are the days of emails from Nigeria with poor grammar and spelling. Today it can be very hard to tell if an email or SMS is not from the real organisation of which you are a customer. Mobile phone numbers are hijacked, legitimate invoices are intercepted, and payment details changed, even bogus parking tickets (armed with seamless ways to pay your fine) are appearing on windscreens.

And this is before "deep fakes" are considered – during the forum we heard about how it can take as little as 3 to 5 seconds of you talking in order to take a voice print and synthesise your voice to conduct a scam over the phone.

It's not just about $$$

Whilst the media focusses on the financial loss, there is far more at risk for both consumers and businesses including trust, reputation, embarrassment and even heartbreak.

A collective problem for consumers, businesses, regulators and law enforcement OR "A bank, a telco, a retailer and a regulator walked into a bar..."

A collective problem requires a collective solution, and momentum is building. This includes initiatives for which a number of attendees at the forum are responsible.

Quantium Telstra, launched in 2023, and CBA have joined together Australia's largest telco (already stopping 332 million scam messages in a month) and the largest banking customer base to reduce the incidence of phone scams. The initiative is designed to detect certain high-risk scam situations in real time, using a Telstra API that CBA will call on as part of its scam detection processes.

This enables CBA to check if a customer is on a phone call – the prime indicator that a scam is occurring. This allows CBA the opportunity to try to contact the customer or put in additional checks. To protect the privacy of both parties, CBA is only able to access specific data points relating to scam prevention through the API and does not have access to any other underlying customer data.

Of great interest was the position Telstra and CBA expressed that the solution they are developing should be extensible to all competitors within their respective business categories – to be most effective the whole industry needs to be "in" (and to enable, regulators need to be "facilitators" to allow competitors working together in the national interest – which is why the ACCC has an "authorisation" team).

The added benefit of a whole-of-industry approach is that competition can be maintained as the concurrent "hardening" of the "small end of town" avoids customers shifting business to larger, better resourced providers whom they may consider to be more secure…

And amongst other initiatives:

- Treasury included a section on scams in the recently published Strategic Plan for Australia's Payments System (https://treasury.gov.au/publication/p2023-404960)
- The ACCC launched the National Anti-Scam Centre in July 2023
- Banks are backing industry wide initiatives such as speeding up communications before funds are lost forever, and ASIC is now undertaking consultation with industry on scam avoidance, management and mitigation, and
- The AFCX is making attempts to become less "banky" by extending membership to 2nd tier banks, crypto exchanges and telcos.

Key themes from the forum

1. Friction

Whilst there were various descriptions of how to approach the issue, a key theme was introducing friction into the system in an environment where we want real time, but not when we are being scammed - the reason racing cars have great brakes is to allow them to go really fast...

Infrastructure friction – industry collaboration and sharing, facilitated by regulators, to introduce safeguards in the infrastructure stage. The Telstra-CBA partnership, the broadening of the AFCX membership and the preparedness to allow competitors to share in prevention strategies and platforms are all good initial examples.

Instruction friction – education and creating awareness to introduce friction leading up to, and at the point that a consumer is potentially authorising a payment to a scammer. Think carefully if something seems too good to be true! And, we must work to remove the stigma associated with being scammed. The National Anti-Scam Centre reported that 30% of scams go unreported and, of those that are reported, it is a significant (but less than 50%) of consumers who consent to their data to be shared for scam prevention and reporting efforts.

Post-instruction friction – looking for the scam and acting faster, and past the first account receiving the money.

2. Collaboration

Industry wide and cross industry communication and data sharing is the optimal way to be able to identify likely scams and, after a scam has been perpetrated, preventing more customers from becoming victims.

3. Taking responsibility

All parties, including the customers (for whom education is priority #1), need to take responsibility for their own behaviour from avoiding a scam in the first place, to adding security and (seamless) speed humps to the payments experience. It should be noted that some scam targets, for example senior citizens, may be less accessible via digital channels, and old fashioned pamphlets and newspaper articles may be needed to reach them.

For example, Barclays Bank in the UK has a pamphlet entitled "The Little Book of Big Scams", which is available on stands in their branches and uses straightforward wording & illustrations in order to educate their customers (as well as using all of its digital channels).

4. Keep planning for the future

Including determining how Digital ID may be part of our solution.

Endnote - A case study from the UK … the Authorised Push Payments (APP) Scams Voluntary Code

Just to pre-empt, the forum group felt that the UK "bank liability" model had not been a successful solution, and the authorities in Australia are on record that this financial liability is unlikely to be a directive for Australia…

Australia has looked towards the performance of the Authorised Push Payment (APP) scams voluntary code introduced in 2019 that provides protections for customers by providing a significant commitment from all signatory firms to reimburse victims of authorised push payment fraud in any scenario where the customer has met the standards expected of them under the code. Where consumers demonstrate that have made reasonable effort to avoid being scammed, banks have agreed that they will take responsibility and reimburse their customer.

In 2020, £147.0 million of losses were reimbursed to victims under the APP, accounting for 47% of losses in these cases. This is up from 41% of losses being reimbursed in cases assessed under the Code in 2019, and more than double the 19% of APP losses that were reimbursed before the Code was introduced.

Here are some of the initiatives that have been undertaken in the UK:

- Development of the "Economic Crimes Plan"
- Establishment of the "Banking Protocol", allowing bank staff to advise police when they think a customer is being scammed
- Fully funding a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), preventing an estimated GBP20 million in fraud and the arrest of 122 suspected fraudsters
- Working with text message suppliers to block suspicious messages
- Working with the regulator Ofcom to crack down on number spoofing, including creation of the "do not originate" list
- "Don't be Fooled" campaign targeting students and young people about giving out bank details and being recruited as money mules
- MITS "Mule Insights Tactical Solution" – software that helps track suspicious payments and identify money mules
- Working with Pay.UK to implement Confirmation of Payee, an account name-checking service that helps prevent authorised push payment scams.
- Fraud awareness campaigns such as "Take five to stop fraud".

About the author
David Ojerholm

David has 40 years experience in financial services and over the last 6 years has specialised in payments as Partner at The Initiatives Group. His career includes being a founder of Pinpoint, that grew to provide loyalty programs to 25 banks, their 100 million customers and 50,000 merchants, eventually being acquired by Mastercard to become their global loyalty business. Prior to that David worked at Westpac and American Express.

Expert Participants

Moderator

Paul Franklin
Independant

Speakers

James Roberts
CBA

Julia Steward
Amazon

Sandy Cameron
Quantium Telstra

Richard Flemming
ACCC

Ben Scott
Idemia

Holly Dorber
PayPal

Saket Narayan
Amazon Web Services

Sharon Skariah
Stripe

Nick Davidson
EY

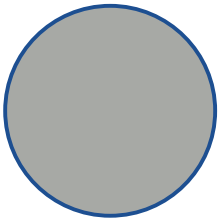
Rob Tesoriero
FIS

Aidan O'Shaughnessy
AP+

Max Alves
PoliceBank

Rajat Jain
Auspaynet

Sanket Bhat
Xero



Anna Zhou
Commonwealth Treasury

Peta Gray
NSW Treasury