



Preventing fraud in a real-time world

Cuscal NPP White Paper No.3

Authors: Nathan Churchward, Senior Manager, Payments;
Michelle Trundle, Senior Manager, Fraud

Cuscal 
The complete payments partner

Contents

Introduction	03
Lessons learned from the UK	05
Understanding the threat	06
Addressing the problem	09
Moving ahead with confidence	13

When the New Payments Platform arrives, it will position Australia as a global leader in real-time payments.

As exciting as that is, as a financial institution there are an array of practical considerations that you need to take into account. Key among them is managing the potential for fraud. While fraud prevention may seem like a daunting task, in Australia we are well positioned to do so.

Our existing services, such as “pay anyone,” are already well established, and we lead the world in smartphone adoption. That’s significant because smartphones offer greater opportunity for security and identification, including in-app messaging and biometrics. We also have the benefit of being able to draw on key learnings from those who have gone before us in real-time payments. By studying the experiences of countries like the UK, for example, we can glean important insights and apply them here.

Another advantage that we now have is the power of machine learning and artificial intelligence. Although the technology was in its infancy when many other real-time payment schemes were launched, in the years since it has made major advances. Today, it’s a highly effective tool for thwarting would-be fraudsters.





To minimise that potential risk, it's essential that you are ready when the NPP goes live.

Yet as we will see, when it comes to preventing fraudulent activity on a fast payments system, it's not merely a question of learning from others or taking advantage of the latest technology.

Equally, if not more important, is recalibrating your approach to fraud by increasing your focus on planning and prevention. The reason is simple: While fraud in an NPP world is likely to be just a variation of what's already occurring today, it's going to happen much faster. In a paradigm where transactions are completed in seconds, there simply won't be time for traditional detection methods.

The good news is that by learning from others and taking the right steps, we will be well placed to minimise the chances of fraudulent activity occurring through the NPP. Key among those steps is proactively educating and preparing all of the relevant stakeholders.

In this paper, we will outline the key considerations that you need to be aware of around fraud and explain what the NPP and Cuscal are doing to help prepare.



The reality is that although the NPP isn't inherently riskier than our current payments system, you still need to be vigilant. Fraudsters are always looking for new opportunities to make money, so could be waiting for the NPP to go live to try to test how secure it is. To minimise that potential risk, it's essential that you are ready when the NPP goes live.



Lessons learned from the UK's Faster Payments Service

When the UK launched its Faster Payments Service (FPS) in May 2008, it revolutionised the banking industry there overnight. While overall fraud did not increase significantly, in the weeks and months that followed, there were a number of instances of fraud at one particular bank. The reason? Transaction security wasn't as prevalent then as it is now. The bank's fraud detection systems were predicated on having hours to authenticate and validate transactions and they just weren't ready for real time. As a result, a handful of fraudsters were able to temporarily exploit this weakness.

Another reason is that there were high daily transaction limits for financial institutions when FPS was introduced, so when fraudsters found an opening they were able to significantly exploit it. In Australia participating financial institutions will be able to set their own customer transaction limits, allowing NPP payments to grow safely as the industry grows confident with the risk profile.

The lesson from the UK example is clear: While good preparation is critical, so too is experience. Fortunately, over the past decade, Australia has collected a wealth of transaction security experience that will help us avoid similar issues.

Understanding the threat

There's a common perception that the speed of real-time payments will increase the risk of fraud and leave customers more vulnerable to attack. In reality, however, things aren't that simple. Fraud is a challenge that every industry faces and is trying to prevent. That means there are lots of different ways to solve the problem, many of which are well-suited to real-time payments.

With this increased focus on fraud prevention, and the lessons we have learned from the introduction of real-time payments in other countries, Australia's financial services industry is in a strong position.

And, let's not forget that to connect to the NPP as a financial institution, you effectively have to have real-time fraud controls in place. Everyone from regulators to customers expect financial institutions to use real-time fraud controls to meet the needs of a real-time payments environment.

Australia's financial services industry is in a strong position.



Plus, not only do Australian financial institutions have very good fraud prevention and detection capabilities, they also have excellent visibility into their customers' typical payment patterns, which is critical for fraud prevention. That's due in large part to the amount of collaboration taking place. Financial institutions regularly work with each other, for example, and Australian financial crime investigation and enforcement agencies to identify and prevent scams and other fraudulent activity.

Importantly, all of this know-how is being applied to the NPP. For instance, there are rigorous verification standards around the creation of PayIDs to deliver confidence in the service and provide payers with confirmation of the payee. And, to help banks monitor payments with greater certainty, each payment includes the actual account name of the payer. On top of this, as part of the 'push' nature of NPP payments, each payment is authorised by the account holder. This is in contrast to other types of payments, for direct debits or credit card payments, where there's an assumed authority when a payment is debited from the account.

Although real-time fraud detection systems are highly effective, and NPP payments will be payer-authorised, the fact remains that scams are unavoidable. The simple truth is that fraudsters will always find new ways to cheat money out of victims.

Active authorisation

The NPP works on the basis that each payment must be approved by account holders. There's no assumption of authority when a payment is debited from an account, as can be the case with other payment methods like direct debits or credit card payments. Instead, the NPP is solely focused on actively authorised payments.



There are three main fraud risks that will have the highest impact in a real-time system that you need to consider:



1. Social engineering scams or spoofing

When a fraudster manipulates a customer, convincing them to issue a payment in good faith.



2. Account compromises

When a fraudster obtains a customer's sensitive payment data and initiates a payment instruction.



3. Mule accounts

Accounts that look legitimate, but are actually set up to perpetrate fraud or money laundering.

While each of these types of fraud requires careful consideration, according to the UK's Faster Payment Service, social engineering scams are the most common type of fraud in the UK that doesn't involve cards. Typically, they are designed to trick people into:

- Providing their bank account details and online banking credentials to fraudsters purporting to be bank officers and who say that they want to move their funds for safekeeping.
- Sending payments to support seemingly legitimate causes, government agencies such as the Australian Tax Office, or even the UN. Ultimately, however, the funds wind up going to fraudsters.
- Sending payments intended for genuine payees to a fraudster's account using spoofing software or by manipulating invoices.

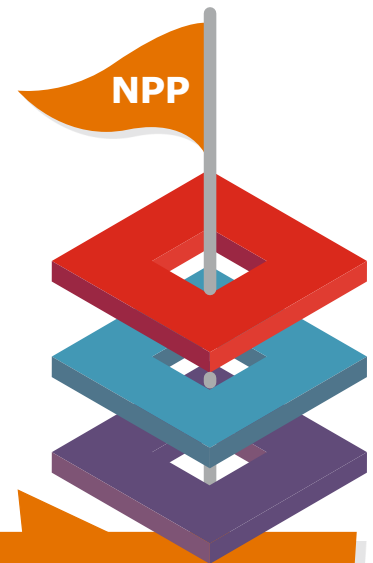
While real-time payments may make Australian bank accounts more attractive to fraudsters, it's important to point out that the risks are generally the same as with current payment methods. Risks and exposures are primarily account based. And, since the transactions are authorised by customers, to make a fraudulent NPP payment a customer's account must first be compromised.



Addressing the problem

Fraud prevention was traditionally a four-step process that consisted of planning, prevention, detection, and response. Given the relatively long lag times associated with traditional payments, the approach generally worked well. Banks had the luxury of time and could detect and prevent fraudulent activity before a payment was processed.

With the NPP, however, payments are going to be processed in seconds. And while as a financial institution you can choose to decline or hold back payments that you suspect are fraudulent, your ability to do so is quite limited. All the more so given that customers will quickly come to expect that their payments are being sent in real time. Practically speaking, that means that in most cases there's no longer going to be time to detect and stop a fraudulent transaction using traditional methods. For that reason, the focus needs to instead shift to planning and prevention.



With the NPP payments are going to be processed in seconds.



There are four main ways to do so:



1. Investing in customer education.

Consider investing in ongoing education to build awareness of fraud scams and risks for your customers. You can also leverage the information and tools provided by the Australian Government's Scamwatch service (scamwatch.gov.au). For an example of a broader instance of customer education, see the UK's "Take Five" campaign (takefive-stopfraud.org.uk).



2. Ensuring strong controls for change of details.

Review your policies and processes for updating customer details. Are your staff aware of the risks and are they verifying all requests for changes or information? When your customers are adding new payees to mobile or internet banking, are you ensuring that the controls on your channels are strong enough to deter fraudsters from accessing and creating their own payments?



3. Implementing PayID verification.

A PayID is a smart address for payments. It links someone's bank account to a recognisable and memorable piece of information the person uses in everyday life, such as their phone number or email address. A PayID can only be linked to one bank account at a time, and is the responsibility of the financial institution that holds the account. As well as a phone number or email address a PayID can also be an ABN or 'organisation ID' such as a company name. In the UK, they have a similar set up that's called Paym, and report no incidence of fraudulent proxy registration.



Take note!

As a financial institution, you are responsible for effectively registering your customers' information in PayID. That's because while the payer normally bears their own loss for authorised fraudulent payments, this rule is subject to exception in cases where a PayID is registered fraudulently or erroneously.

For that reason, you need to take particular care, both when the NPP launches and you are registering PayIDs in bulk, and subsequently any time that you need to make changes to your customers' information. The most important control is for the name that is used with the PayID. Ensure your systems maintain this appropriately and fraudsters cannot nominate a name that does not represent the account holder or their account name.



4. Continuing to collaborate with financial institutions and others.

It's important to note that responsibility for fraud prevention can't lie solely with the NPP. As a payments industry participant, you need to do your part too, which might consist of any combination of:

- Protecting the front door using biometric log-ins, device fingerprinting, and other tactics such as two-factor authentication.
- Using real-time detections, pattern screening and quarantine for investigation.
- Conducting data analysis and sharing blacklisted PayIDs and payee accounts.

Perhaps most important of all, it's critical that you ensure that your own fraud detection and prevention systems are state of the art and effectively protecting your business. Those systems will do much of the heavy lifting on your behalf.

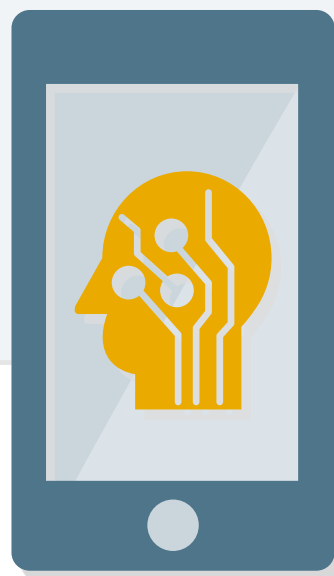
Spotlight on artificial intelligence

In today's digital age, financial institutions and retailers are increasingly relying on big data and artificial intelligence to prevent fraud. With rapidly changing fraud trends, and new types of fraud cropping up all the time, rules-based systems simply cannot keep up. By combining machine learning with human intelligence, many organisations are developing data-driven fraud systems that are capable of predicting and preventing losses before they occur, and giving valued customers the ability to transact without interruption.

In fact, integrated fraud management platforms respond in real-time, using artificial intelligence to display intuitive reasons for a human to make sound decisions and respond to fraud effectively. This is in contrast to traditional reactive platforms which require a fraud agent to perform lengthy data searches for investigation. Systems are able to process large amounts of data and complex algorithms in real time, without sacrificing the real-time authorisation response times that are essential in real-time environments.

While even the most sophisticated machine learning platforms still require human intervention, the real value they offer is their ability to process large amounts of information in seconds. They also learn from the inputs from fraud intelligence agents and can be used to detect new fraud patterns and other suspicious events that might otherwise go undetected using a rules-based system. They do this by continuing to track and update metrics on individuals, events, and channels, performing complex analytics to differentiate between good transactions and those that you would either want to block or refer to a specialised fraud agent for further investigation.

While financial institutions are working to reduce and prevent fraud, this needs to be balanced with customer experience. Fraud systems that can profile at an individual level are able to maintain very low false positive ratios which allows genuine customers to transact in a frictionless manner. These type of systems will be very effective in a real-time environment.





Moving ahead with confidence

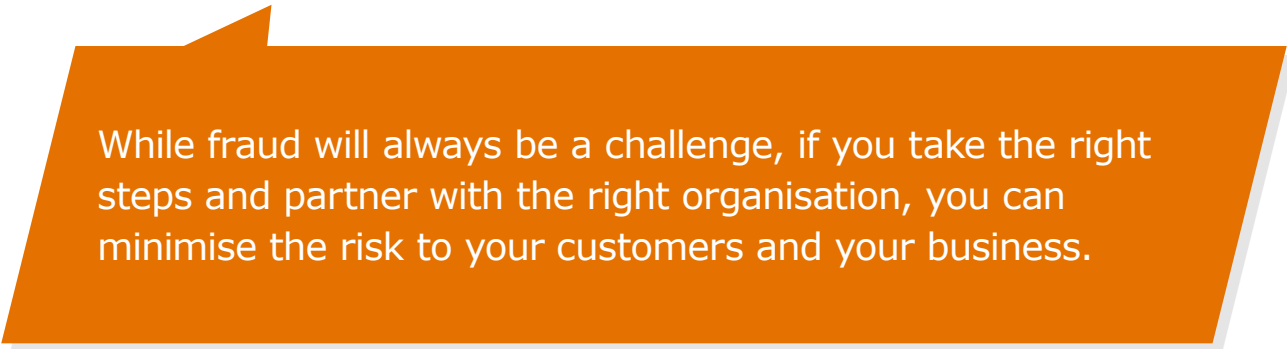
The NPP will soon make real-time payments a reality in Australia. And while that represents both opportunities and challenges, it's certainly nothing to fear.

The reality is that although there is a lot of attention being given to risk, the risks associated with real-time payments are the same ones that have always existed. Speed is the only new part of the equation, but even that isn't something for you or your customers to be worried about as long as you are prepared.

By taking a holistic approach to risk management — one that encompasses both your own internal controls as well as the robust real-time transaction monitoring that third parties like Cuscal can offer — you can have the utmost confidence in real-time payments. While fraud will always be a challenge, if you take the right steps and partner with the right organisation, you can minimise the risk to your customers and your business.

We're very proud to be working with Feedzai for our central fraud hub. The company was founded and developed by data scientists and aerospace engineers, and provides an advanced risk management platform leveraging big data and artificial intelligence. That fraud hub has been designed with our clients in mind to complement their existing systems. This will allow them to use the NPP with confidence from day one, bringing an array of new benefits while minimising risks.

That's a win-win by any standard, for our clients and their customers.



While fraud will always be a challenge, if you take the right steps and partner with the right organisation, you can minimise the risk to your customers and your business.

To find out more about Cuscal please visit

www.cuscalpayments.com.au

Cuscal 
The complete payments partner