New payments platform

The industry approach to minimising real-time payments fraud

KPMG.com.au | nppa.com.au

Executive summary

The New Payments Platform (**NPP**) is new, world-leading domestic payments infrastructure that enables connected Australian financial institutions to offer their customers – consumers, businesses and government agencies – near real-time, data-rich inter-bank payments 24 hours a day, 7 days a week. The platform launched to the public on 13 February 2018.

It is an open platform that is designed to support multiple overlay services which could be offered by a range of service providers from the fintech and financial services community, or from any other sector outside of the traditional payments industry. It is in this 'layering' of the architecture that the NPP offers opportunity for future innovation and development.

The NPP's distributed architecture design is the result of intensive industry collaboration over several years, between the Reserve Bank of Australia (**RBA**) and Australian financial institutions – large and small – to design and build a secure platform for domestic payment services that meets the needs of Australia's digital economy. It is arguably one of the most significant pieces of national payments infrastructure to be built in Australia in decades.

This paper considers the fraud risk, and the potential impact to fraud risk, of real-time payments.

Fraud risk is a particular operational risk in any payment system, but is frequently cited as being a higher risk in real-time payment systems due to the velocity of payment processing, and the typically irrevocable nature of real-time payments.

Real-time payment systems have been operational around the world for many years, and while data about online banking fraud by service or payment type in those countries is not generally publicly available, many commentators point to the UK implementation of real-time payments in 2008 as evidence for the proposition that faster payments inevitably lead to an increase in fraud. This tends to beg the question whether faster payment systems create *new* fraud risks.

Experience suggests that real-time payment systems do not create new types of fraud – the typologies of account compromise are consistent across both traditional and real-time payments systems. However, the velocity of payment processing *does c*hallenge financial institutions' fraud detection and prevention tools that were designed and adequate for slower intraday and overnight batch processes.

Unaddressed, this vulnerability could be exploited by fraudsters and scammers.

To meet this challenge, institutions with experience in real-time systems attest to the importance of upgrading to leading technology solutions to provide a fraud risk management framework that focuses on identity, authentication and payment monitoring in real-time and consumer education.

Research indicates Australians are enthusiastic adopters of new technology generally, and of digital and electronic banking and payment services in particular. Australian financial institutions have a solid track record of providing safe and secure online and mobile banking applications, that over the last few years have leveraged interbank batch clearing and settlement arrangements which occur several times each business day.

Australian financial institutions already deploy fraud detection for online commerce and real-time online banking authentication tools to protect their customers when they make payments. This, together with Australia's consumer protection framework that ensures consumers are compensated for unauthorised transactions where they have not contributed to the loss, is the context for the Australian implementation of real-time payments.

Thus, whilst the NPP is not expected to create new fraud types, participating financial institutions recognise the particular operational risks of processing velocity and 24/7 operations, including the need for effective real-time technology-based tools to manage banking fraud risks and to help protect their customers from scams. Australian financial institutions further recognise that banking fraud risk is not a static concept and continuously invest in enhanced prevention and detection in line with global markets to stay ahead of new trends in digital fraud.

Australian financial institutions offering NPP payment services to their customers are well-placed to manage fraud and financial crime risks by:

prioritising security authentication controls for online banking to 'protect the front gate', including use of multi-factor authentication, biometrics, device and IP authentication and the consideration of more sophisticated behavioural biometrics;

leveraging a range of advanced real-time fraud prevention and detection controls, including artificial intelligence / machine learning systems and payment pattern monitoring to identify and hold unusual payments for fraud checking;

continuing to proactively roll out consumer education campaigns to increase customers' vigilance around potential scams; and

continuing to promote industry collaboration between financial institutions, regulators and law enforcement agencies to stay ahead of emerging financial fraud trends and scam activities.

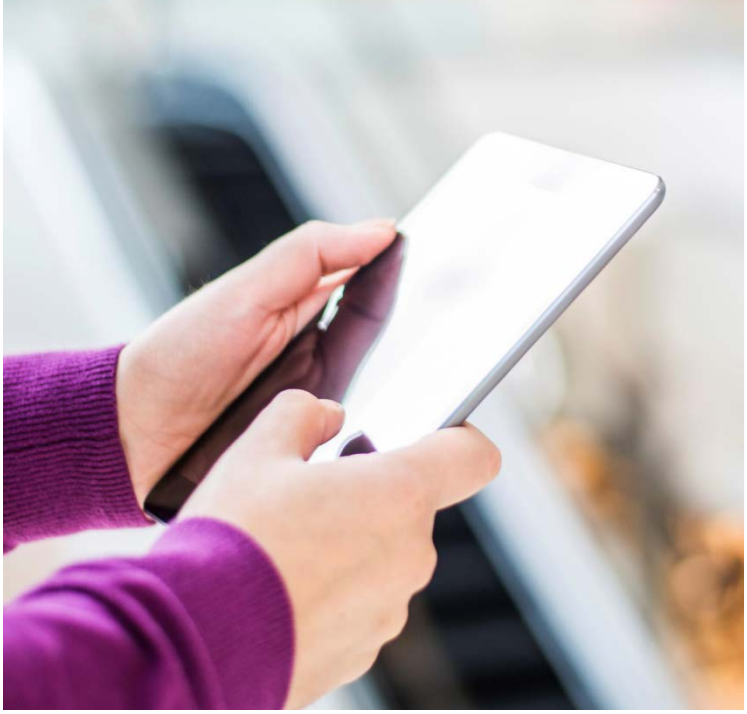
The NPP also includes a new addressing service, named PayID, which allows customers to optionally register their phone number, email address or ABN and a 'display name' in a central secure repository, via their financial institution which is then linked to their bank account details.

A PayID is used to direct a payment into a linked account – it cannot be used to withdraw from that account. A PayID name is recorded with the proxy (email, phone number or ABN) and account details.

The NPP message flows and rules have been designed to enable PayID name validation for all PayID initiated NPP payments. This particular feature will enable payers to check and confirm a payee before authorising a payment, reducing the incidence of misdirected and mistaken payments, including payments to fraudsters and scammers purporting to be a genuine payee.

In conclusion, the NPP has been designed to support innovation and competition in digital commerce and payments services now and into the future. It has also been designed with the benefit of observing faster payment system implementations in other jurisdictions, designing out vulnerabilities and incorporating enhancements to existing systems. The platform is expected to revolutionise the Australian payments industry and fuel the digital economy.

What is the New Payments Platform?



The New Payments Platform (**NPP**) is new, national payments infrastructure for the Australian economy that enables consumers, businesses and government agencies to send and receive real-time domestic Australian dollar payments using either easy-to-remember 'PayIDs'[1] that link to a bank account, or traditional BSB and account numbers. NPP and PayID services offered by participating institutions are built in to consumers' usual mobile and online banking applications, eliminating the need for additional applications to be downloaded.

In addition to the NPP's many benefits for end-users, the platform's architecture and open access enables multiple overlay services to be offered, each leveraging the capabilities of the platform's 'Basic Infrastructure' to offer different products and services, allowing for future innovation and development.

The NPP was established following the Reserve Bank of Australia's (**RBA**) strategic review of innovation in the Australian payment industry in 2012. The RBA (through the Payments System Board) endorsed a proposal developed by the Real-Time Payments Committee for new, real-time payments infrastructure in response to that review.[2] The platform has been built and funded by thirteen financial institutions, including the RBA. It is owned and operated by NPP Australia Limited (**NPPA**), an industry joint venture company that is tasked with overseeing its build, operation, governance and growth.

[1] A PayID can be a person's phone number, email address, ABN/ACN or an unique 'Organisation Identifier'.

[2] The RBA published its conclusions to its Strategic Review of Innovation in the Payments System in June 2012, identifying objectives for the Australian payments industry. In response to the RBA's Review, the Australian Payments Clearing Association Limited (APCA – now Australian Payments Network Limited) established and coordinated the industry committee, the Real-Time Payments Committee (RTPC), responsible for developing a proposal to deliver the 'Core Functions' (being, speed, 24/7 availability, data-rich and simple ad- dressing). The RTPC recommended a new distributed layered business architecture for payments clearing and settlement designed to deliver the highest standards of security, performance, availability and resiliency, with dedicated gross settlement functionality and Exchange Settlement Account management arrangements provided by the RBA to resolve liquidity and credit risks prevalent in domestic payment systems.

Authorised deposit-taking institutions (**ADI**s) regulated by the Australian Prudential Regulation Authority (**APRA**) are eligible to connect directly to the NPP via distributed payment gateways (**PAG**s) for the purposes of clearing and settling NPP payments. These connected ADIs are also able to offer indirect access to the NPP to other financial institutions and corporate users that do not wish to, or are ineligible to, connect directly.

At its core, the NPP is comprised of three main components:

The Basic Infrastructure

Includes a network that connects participating financial institutions, a switch that moves messages between them via the network and an addressing service, named PayID.

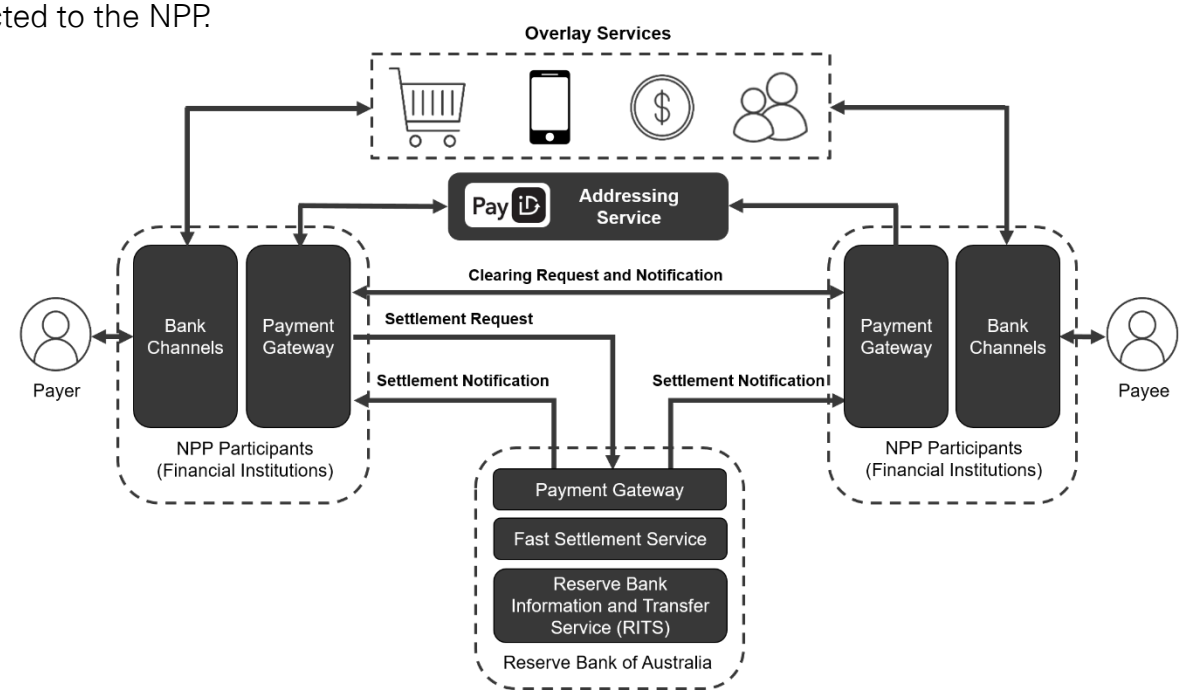
The Fast Settlement Service

A component of the Basic Infrastructure provided by the RBA that allows cleared NPP payments to be settled in real-time by debiting and crediting the Exchange Settlement Accounts (**ESA**) of the two financial institutions that are acting for the payer and payee customers. It is the settlement finality in the ESA funds that effectively enables the posting of value to customers account within seconds.

Overlay Services

Overlay Services are the payments-related products or services that leverage the Basic Infrastructure. This is where the NPP can open the door to innovation and competition in the payments space by providing opportunities for overlay service providers to develop value-adding payment-related services and solutions. The first Overlay Service to go live on the platform was Osko by BPAY. Its first phase allows consumers to send real-time payments with payment descriptions of up to 280 characters.

Figure 1: Depicts the NPP message and information flows between financial institutions directly connected to the NPP.



Why do we need to innovate in the payments space?

Faster payments systems have been operational around the world for many years, including in the United Kingdom[3], Singapore[4] and more recently, the United States[5]. The RBA's strategic review in 2012 observed that whilst Australian business and consumers were at the time well served by digital banking and payment services, with some segments of the market also having access to aspects of real-time payment services and value, the capability was not ubiquitous. From a public policy perspective, it was considered that real-time interbank transfer functionality, along with messaging standards that enabled transmission of richer remittance information, ability to transact outside normal business hours and an addressing solution would address a number of gaps in the domestic payments landscape and would provide a sound basis for innovation, efficiency improvement and competition in payments services.

Australians are enthusiastic adopters of new technology generally,[6] and of digital and electronic banking and payment services in particular.[7] Customers of financial institutions connected to the NPP will be able to make and receive real-time payments. Under the existing low value direct entry payments system[8], payment messages are batched and exchanged between financial institutions five times each business day, with settlement occurring throughout the day. Depending on the timing of the payment (weekends and public holidays) and the cycle of interbank clearing and settlement, direct entry BECS payments can take anywhere from a few hours to 2-3 days to appear in a recipient's bank account. The opportunities for maximising efficiency presented by the move from intraday batch payments to real-time cannot be underestimated, and are a key driver for the move to faster payment systems around the world.

[3] UK FPS launched in 2008: www.fasterpayments.org.uk (accessed 16 January 2018).

[4] Fast and Secure Transfers (FAST) launched in Singapore in 2014: www.abs.org.sg/fast.php (accessed 16 January 2018).

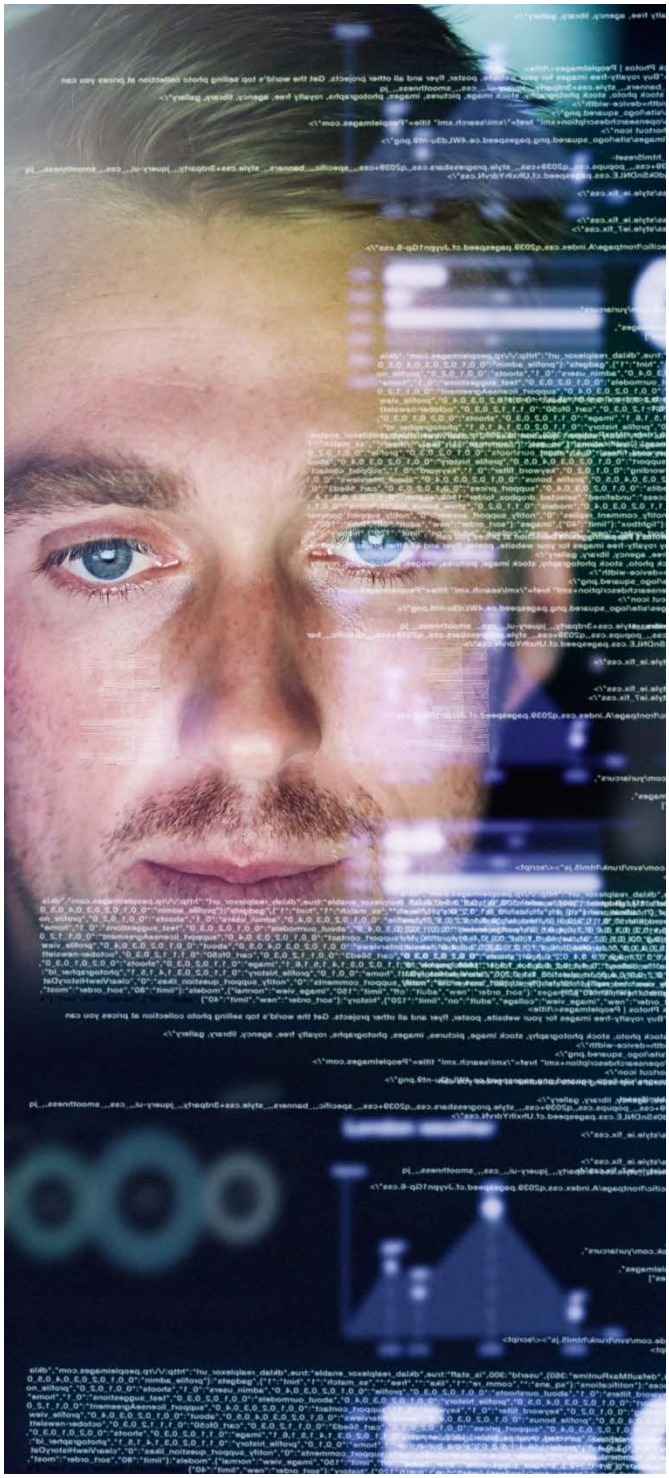
[5] Real-Time Payments (RTP) operated by The Clearing House launched in the USA in November 2017: 'First New Core Payments System in the U.S. in more than 40 Years Initiates First Live Payments', The Clearing House, 17 November 2017, www.theclearinghouse.org/press-room/in-the-news/20171114%20rtp%20first%20new%20core%20payments%20system (accessed 9 January 2018).

[6] Australia continues to be one of the leading smartphone markets globally, with penetration at 83 per cent in 2016 and forecast to increase to 89 per cent in 2019, http://www.bandt.com.au/marketing/zenith-report-australian-smartphone-penetration-reach-89-2019 (accessed 4 March 2018).

[7] In 2016, 56% of respondents to an RBA survey had made at least one online payment during the survey week (double the amount since 2007): https://www.rba.gov.au/publications/rdp/2017/pdf/rdp2017-04.pdf

[8] Bulk Electronic Clearing System (BECS) administered by the Australian Payments Network

Is fraud an issue with faster payments, and how will it be tackled?



Faster payments systems are often perceived as riskier than traditional electronic payment systems due to the velocity of payment processing and the challenges of fraud and scam detection and prevention in real-time. Financial institutions have less time to detect unusual transactions compared with traditional payment systems, which means they need to invest in effective real-time controls.

Fraud and scam risks, however, exist in all payment systems, including credit cards, cheques and online banking. *Figure 2* sets out the existing types of banking fraud and scams. Banking fraud, or unauthorised transactions, occur if a customer's account is compromised and transactions are made without the customer's knowledge. Scams, on the other hand, occur when a person is tricked into authorising a payment to a fraudster or revealing bank account details and passwords to a fraudster through social engineering or phishing scams – for example, scammers target and convince people to make payments to them with 'get rich quick' investment opportunities, offers of unexpected winnings that will be released with 'just a small payment', fake charities or similar schemes designed to convince a person to send a good faith payment to a scammer.

The terms 'fraud' and 'scam' are often used interchangeably in the electronic banking context, particularly as phishing scams often target victims' information such as banking credentials which can then be used to access a victim's account. There is no published data about losses due to unauthorised transactions, but data published by the Australian Competition and Consumer Commission (**ACCC**) Scamwatch indicates that losses due to scams are significant and have been growing year on year.

Figure 2: Banking Fraud and scam types

	Cards	Cheques	Bank account fraud
Banking Fraud	**Card not present fraud.** 'Card not present' fraud occurs when debit or credit card details are stolen and used to make an unauthorised purchase or payment without the card, for example, online or by phone. Card not present fraud made up 78% of all fraud on Australian cards in 2016.[9]	**Cheque fraud.** This involves fraudsters altering cheques or stealing or counterfeiting cheques.	**Application Fraud (using identity theft).** This involves using someone's identity to open bank accounts to procure credit cards or loans, steal money or for use in other criminal activity. Identity theft can take many forms but essentially involves compiling personal data – e.g. from stolen documents, data compromised in cyber/data breaches to establish the 'authenticity' of an assumed identity.
	Card present fraud. This involves fraudsters stealing a person's credit or debit card to make unauthorised purchases at point-of-sale devices, or to withdraw money via an ATM using a stolen PIN.		**Account compromise / takeover.** Fraudulent account compromise involves the use of stolen online banking credentials (bank account details and password) to effect credit transfers in an authenticated banking session. Fraudsters use hacking and phishing/social engineering scams to gain access to banking credentials.
	Counterfeit cards. This involves fraudsters producing counterfeit cards using skimmed details from the magnetic strip on a credit or debit card.		**Hacking.** This involves exploiting security weaknesses on electronic devices or networks to commit identity theft and banking fraud. For example, hacking to gain access to banking credentials or modifying of an attribute (such as the account number or transaction amount) of a genuinely issued payment instruction
Scams	**Scams.** A scam is generally any manipulation of a person by the fraudster which results in the person making a good faith payment to the fraudster's bank account or to a mule bank account or providing the fraudster with banking credentials and passwords to commit account compromise. Scammers can target and trick people with: the classic 'get rich quick' investment opportunities that sound too good to be true, offers of unexpected winnings that will be released with 'just a small payment', fake charities, using fake dating profiles playing on emotional triggers to procure money, gifts or personal details that can be used to commit identity theft, and more recently, 'CEO scams' that are designed to trick a person in a business organisation to send a payment to a scammer (posing by email or SMS as the boss). All scams involve individuals (and sometimes business organisations) being tricked into making a payment (which could be via an electronic payment to an account, iTunes cards posted to a post office box or overseas remittance services) or handing over gifts or information that can be used to compromise the victim's accounts.		

[9] Australian Payments Fraud 2017 (Jan-Dec 2016 Data), Australian Payments Network.

Banking fraud – secure banking applications; 'protect the front gate' and continuous authentication

Faster payment systems do not introduce new types of banking fraud, but may create challenges for financial institutions that assume traditional fraud prevention and detection tools will be fit for purpose in the real-time environment.

Commentators often point to the United Kingdom's apparent increase in banking fraud between 2008 and 2009 following the launch of Faster Payments Service (**FPS**) as evidence of the inherent risk in real-time payments[10].

While there is conjecture about the relevance of the data, and debate about the cause of the apparent increase in online banking fraud at that time, former Royal Bank of Scotland Managing Director, Kevin Brown, explained the UK fraud experience post-FPS as follows:

"The initial fraud experience in the UK was shaped by the services/technology at the time of launch. The UK Faster Payments Service went live at a time prior to the mobile/app banking services we see today and also before two-factor authentication was rolled out fully in all channels/client segments. There was also a significant challenge in the quality of Know Your Customer (KYC) information in many banks. At implementation, alongside the introduction of upgraded payment monitoring/proofing systems, the majority of the UK Banks managed their risk exposure by managing limits on the different channels/client segments e.g. where two-factor security was in place higher limits were allowed whereas situations where partial PIN/Password were used saw lower limits.

The UK Fraud data shows losses of £1.60 per £1000 in 2008 and by 2013 this had fallen to 7p per £1000. Whilst not exclusively, much of this improvement will reflect the full implementation of two-factor security on all channels, completion of 'know your customer' (KYC) remediation, refined payment profiling and a number of continuous security enhancements to protect access to the account and the set-up of new payees, including confirmations via text/e-mail/phone.

It remains a continuous challenge to stay ahead of the fraudsters and the industry and individual banks are always implementing additional protection for customers using both mobile and on-line initiation of payments."

[10] Statistics published by Fraud UK showing 132% in fraud between 2008 and 2009 is not solely based on payments made through the FPS. For analysis, see: Julius Weyman, Federal Reserve Bank of Atlanta, Risk in Faster Payment, 2016, p 16:

> *None of the faster payment schemes makes fraud data publicly available that are specific to the faster scheme alone. Even if such were available, the relative newness of faster payment schemes in most countries would make trends questionable and conclusions premature. That said, general observations about the trends available in the United Kingdom show that at the launch of the United Kingdom's faster payment scheme in 2008, online banking fraud increased 132 percent from the previous year. The 2009 level was 14 percent higher than that in 2008. Following a downward trend in 2010 – 11, online fraud trends have steadily advanced, with the series showing its highest level yet in 2014.*
> *It is impossible to judge the extent to which the faster scheme itself is pivotal to any trend. However, it seems reasonable to conclude that a new scheme will offer new security challenges. It also seems prudent to keep things in perspective.*

Ten years post-FPS implementation in the UK, online banking controls and transaction authentication processes used by financial institutions around the world have come a long way. Recent implementations of faster payment systems have tended to show that with effective identity access management and transaction monitoring processes in place, and with ongoing enhancement of fraud prevention and detection to stay ahead of new fraud schemes, the impact of real time systems on overall banking fraud rates can be minimal.

Australian financial institutions, as well as banks in many other jurisdictions, employ a combination of multi-factor authentication and biometrics, such as fingerprint and voice, to 'protect the front gate' from account compromise and sophisticated fraud detection tools to monitor and minimise the risk of unauthorised payments being made from their customers' accounts.

Financial institutions that send NPP payments are expected to step up implementation of emerging and innovative technologies designed to prevent and detect fraud in real-time and leverage behavioural biometrics, artificial intelligence machine learning and monitoring of customer payment patterns against dynamic customer profiling to help identify and stop unusual transactions with a higher fraud risk profile. Other tactics we might expect Australian financial institutions to deploy include holding NPP payments to a first-time payee, or imposing a daily limit or an individual transaction value limit on payments.

If, despite these endeavours by financial institutions, an individual customer suffers loss due to an unauthorised transaction, common law and industry consumer protections are in place to protect and compensate where it is clear that the customer has not contributed to the loss (for example, by disclosing their secure banking credentials and passwords).[11]

Scam vigilance – account monitoring and customer education

Data published by the ACCC shows that reported scam losses rose by 8.8% between 2016 and 2017 to a total of $90.9 million[12] with phishing scams becoming increasingly sophisticated and targeted. It is important for consumers to be vigilant about scams, particularly scam payments sent via faster payment systems as recovery can be difficult unless the scammer's financial institution is put on notice and is able to freeze their account before funds are transferred out.

To protect their customers, financial institutions may also use their real-time fraud detection tools to monitor accounts for unusual transactions that may reveal that a person has fallen for a scam – for example, if a customer does not normally make large or frequent payments or send money overseas, their financial institution may consider this type of activity unusual and contact them to investigate whether they have fallen victim to a scam.

However, as effective as banks' real-time fraud detection systems may be, fraudsters look to exploit new opportunities to scam and defraud victims. It is well established that consumer education and vigilance is central to scam protection, and financial institutions will continue to provide information and tips to their customers on how to protect themselves against scams, device compromise and account compromise.

[11] For example, refer to ePayment Code, which is a voluntary code administered by the Australian Securities & Investments Commissions (ASIC). A copy of the Code and a list of subscribers is available at www.asic.gov.au. Refer to the Code for its scope of consumer protections.

[12] ACCC Scamwatch, https://www.scamwatch.gov.au/types-of-scams (accessed 6 February 2018).

In addition to making it easy to address payments, NPP's PayID service is also expected to help to stop some scams occurring as payers who make NPP payments using a PayID will be able to check the name of the recipient linked to the PayID that they have entered before authorising the payment. This name confirmation feature has the potential to minimise payments being accidentally misdirected, as well as maliciously misdirected to scammers who purport to be someone else, like the Australian Taxation Office or an employer. PayID may also alleviate some payee customers' concerns around having to share sensitive BSB and account information to receive payments.

To ensure the highest level of security, registration of PayID information in the addressing service can only be made by a customer's financial institution. Institutions that register PayIDs are required to comply with robust registration and authentication processes to prevent erroneous or fraudulent PayID registrations.

The NPP rules establish a framework which supports compensation arrangements for payers who incur a loss as a result of a registering institution's failure to comply with these strict processes. It is worth noting that to date, 'PayM', a similar addressing service operated as part of the UK's FPS since 2014, has confirmed that it has not reported any instances of fraud effected by misappropriated or fraudulent proxy registration.[13]

Industry collaboration and collation of analytics

Industry collaboration is an important tactic for staying ahead of emerging fraud trends. NPPA brings together leading security and fraud experts from each of the participating banks to collaboratively manage, monitor and undertake activities aimed at combatting any NPP-related fraud.

NPP participating banks also work closely with regulators, law enforcement agencies and each other, through the Australian Financial Crimes Exchange (**AFCX**) and various other industry fora, to share intelligence and trends in fraud activity and devise solutions to close down fraudsters and scammers as early as possible in the commission of their crimes.

Further, NPPA works with participating banks to share information on emerging scams to help prevent and detect losses and collect data and statistics to understand the types and volume of NPP fraud and scams.

[13] Statement provided by PayM spokesperson on 16 February 2018.

Data Security and Privacy

In addition to the fraud controls discussed above, data security, privacy and cybersecurity risks in the NPP context have been extensively considered and controlled. NPPA and participating banks, together with SWIFT have designed the platform and the addressing service to conform to the highest data and system security standards, and have put arrangements in place to ensure the central infrastructure is monitored and secured against unauthorised access by third parties. In addition:

- data in NPP payments, including payer and payee account details and values, are sent directly from the payer bank to the payee bank via their respective PAGs, and are not copied or stored in any systems managed by NPPA's central repository;
- NPPA prescribes, as a condition of connecting to the platform, the minimum security requirements for any organisation connecting to the NPP. These security requirements apply to both the NPP components that such organisations use to connect to the NPP and their back-office systems; and
- any personal information stored in the addressing service such as BSB and account numbers, customer names and PayID values is collected, encrypted, stored, used, disclosed and managed in accordance with privacy legislation and Australian privacy principles. Encrypted PayID data in the addressing is held in a highly secure environment which is monitored 24/7 and only PayID name details are made available to payers, in accordance with the terms of the PayID owner's consent.

[14] S.W.I.F.T Domestic Australia Pty Ltd. SWIFT website: https://www.swift.com/

Conclusion

The New Payments Platform is designed to meet the evolving needs of the Australian economy by giving financial institutions a secure and efficient platform to enable the delivery of real-time, versatile and data-rich digital payment services on a 24/7 basis. Its addressing service, PayID, is optionally available to provide a simpler and more convenient way to address payments and provides a mechanism for payers to check the 'display name' of the recipient account linked to the PayID before sending a payment – a feature that is expected to help reduce payments being accidentally sent to the wrong account or maliciously to a scammer claiming to be a genuine recipient.

The NPP has been built with security paramount. Financial institutions connecting to the NPP use a range of tools to effectively manage and minimise banking fraud and scam transactions risks, including multi-factor authentication, and real-time transaction monitoring, as well as transaction value limits and holds on payments to first-time payees.

In line with global markets with real-time payments, Australian financial institutions are expected to use increasingly sophisticated tools including behavioural biometrics, continuous transaction monitoring through dynamic customer profiling and machine learning / artificial intelligence to prevent and detect fraud.

Consumers also continue to have the protections of common law and the ePayments Code if unauthorised transactions occur on their account. NPPA and financial institutions are continuing to educate consumers on the importance of staying vigilant of scams that try to trick them into authorising payments or giving out sensitive banking credentials to scammers. Industry collaboration will also play an important role in minimising scams by sharing intelligence to stay ahead of emerging fraud trends.

The world-class design of the NPP has been informed by observations of implementations of real time payment systems in other jurisdictions, and designing out possible vulnerabilities. The NPP creates opportunities for innovation and competition, and is positioned to transform the Australian payments landscape for the benefit of consumers, businesses and government agencies.

Daniel Houseman
Partner, Management Consulting, KPMG
T: +61 3 9288 6820

Natalie Faulkner
Director, Forensic, KPMG
T: + 61 2 9335 7716

Adrian Lovney
CEO, NPPA
T: + 61 2 8278 9610

Vanessa Chapman
General Counsel and Company Secretary, NPPA
T: + 61 2 8278 9610

KPMG.com.au

May 2018. ACS095962