

# Digital investment

In partnership with NAB

www.afr.com | Friday 18 June 2021

## Businesses must bank on secure future

**Networks** Public and private sectors are strengthening the nation's cyber capabilities, writes Mark Eggleton.

The head of Britain's National Cyber Security Centre, Lindy Cameron, warned in a speech at the beginning of this week that ransomware attacks from criminal networks were now a bigger threat to the United Kingdom's security than online threats from hostile states.

It's an issue recently highlighted in cyber security firm SonicWall's 2021 Cyber Threat report, which indicated ransomware attacks had increased by over 60 per cent globally to nearly 305 million in 2020.

According to the report, ransomware volume is running rampant and in the Asia-Pacific region alone, the number of attacks spiked by 455 per cent.

And the attacks continue unabated, as highlighted at the G7 summit last weekend. There have been several significant recent cyber intrusions affecting many G7 and other nations' critical infrastructure, manufacturing and electronics firms, and hospitals.

These transnational criminal enterprises leverage infrastructure, virtual currency, and money laundering networks, and target victims all over the globe, often operating from geographic locations that offer a permissive environment for carrying out such malicious cyber activities.

Bearing this in mind, in their final summit communiqué, G7 leaders

called on "all states to urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions".

Assistant Minister for Defence Andrew Hastie says Australia is on the front foot with cyber criminals and the Australian Signals Directorate (ASD) is working very closely with law enforcement, the Australian Federal Police, and other intelligence organisations to take down cyber criminal networks.

Hastie says Australia is building a world-class offensive cyber capability that is "going after these cyber criminals online if they are offshore and keeping them off balance".

"The ASD is punching back and we need these cyber criminals to know that we have a very capable set of people who will come after you and rip apart your cyber infrastructure and your business model."

"And we've already got results. The ASD, in a different setting, ripped apart Islamic State online. That was a critical operation and we're going to do the same with cyber criminals offshore who are using ransomware to attack Australian businesses," Hastie says.

Forming part of the nation's offensive strategy has been the establishment of top secret joint cyber security centres in capital cities (excluding Hobart and Darwin), which are under the control of the Australian Cyber Security Centre. A collaboration between business and government, the centres are kitted out with classified surveillance systems designed to research and share threat intelligence with and from business in real time right across the country.

For Hastie, the whole point of the joint cyber security centres is "to get government and industry collaborating and understanding the threat and then



The G7 called on all states to 'urgently identify and disrupt ransomware criminal networks'.

working out best practices to keep our businesses safe".

"The main priority for the government is to ensure every Australian is cyber-aware and doing basic things like uploading and patching security updates, using complex passwords or phrases, multifactor authentication as well as backing up their data."

"These are very simple things, but we need everyone doing them."

NAB chief technology and operations head Patrick Wright agrees the simple things such as updating your iPhone or your Android device, "doing the continuous security updates on your laptop computer are really important parts of what we think are good corporate hygiene and good individual hygiene".

"Every day we discover new vulnerabilities and literally billions of lines of code that run the devices that surround us and if you haven't updated your software, your iPhone or changed your passwords, you should be alarmed because there are people actively buying

and selling user IDs and passwords on the web, every day," Wright says.

The only representative from banking on Home Affairs' cyber security industry advisory committee, Wright is confident Australia is on the right path

### ■ The ASD is punching back and we need these cyber criminals to know.

Andrew Hastie,  
Assistant Defence Minister

when it comes to addressing cyber security threats because business and government are working together.

Importantly, Wright understands the challenge facing the nation's small business sector when it comes to mitigating against cyber risks because it's another impost on already tight budgets.

"It's one of the reasons we provide free

software to our clients on our website. We think it's important to talk to them about what we're doing and how we can help them and what steps they should be taking on a more basic level to educate themselves because in many cases, they just don't know the basics of how to protect themselves," Wright says.

NAB spends over \$100 million a year on running and improving cyber security and the threat grows every year.

According to the bank, it blocked 489 million cyber threats in the last quarter of 2020 alone.

Wright says the bank has hundreds of people working on security and works with locally founded but Silicon Valley-based crowdsourced security platform Bugcrowd, who also partner with the Cybersecurity and Infrastructure Security Agency (CISA), a federal agency of the US government.

"We care deeply about ensuring that our customer's data is kept secure, and we work tirelessly to ensure that it is. We

**Continued next page**

## WE BRING BIG IDEAS AND CAPITAL TOGETHER

We're focused on connecting borrowers and investors around the world.

Our Corporate & Institutional team can help with your big idea.

🔍 NAB Big Ideas

more  
than  
money





# A new asset class is shaping up

## Digital infrastructure

Christopher Niesche

The huge upswing in demand for technology and data storage is underpinning the attractiveness of digital infrastructure as a growing asset class, says Rodney Wallis, an executive in the resources, infrastructure and government group at National Australia Bank.

Digital infrastructure assets, in particular data centres, mobile phone towers for wireless networks and fibre optic networks, have emerged as a distinct asset class in recent years as investors seek opportunities in the physical assets that underpin the digital economy.

"This is a capital-intensive industry and continued investment from both the government and the private sector will drive the country's prosperity as almost every aspect of modern business and our livelihoods is becoming increasingly reliant on connectivity," he says. "This will only lead to more opportunities for our investors."

As the digital economy has grown and matured, investors have become aware of the practically exponential growth in demand for connectivity, be it through towers or fibreoptic networks, and in demand for data centre storage as business and government move more operations to the cloud.

"There's certainly a growing awareness of the fundamental underpinning of demand for data, which has meant that in respect to a variety of different opportunities, whether it's data centre-related or towers-related or network-related, there is a growing level of comfort around the predictability and the defensibility of these cash flows," Wallis says.

"There has been a lot of capital invested into the sector and certainly there's only a growing appetite across our investors to continue to invest in the space."

Global private investment in digital infrastructure and telecoms has grown rapidly from less than \$US1 billion in



NAB executive Rodney Wallis, top right, sees opportunities in digital infrastructure. Investors are pouring billions into data centres and digital network centres.

2010 to what we now estimate to be in excess of \$US90 billion per year, Wallis says.

NAB is helping a wide range of investors enter the space, with either bank or debt capital markets funding, as well as with services such as foreign exchange and interest rate hedging.

Digital infrastructure assets provide different opportunities for different investors, says Wallis.

For instance, in a data centre, some investors will be seeking opportunities where there are firm long-term customer contracts which will provide more certainty about future cash flows.

Other investors will be prepared to make an investment on the basis that a data centre will be able to grow by securing new customer contracts.

"One of the things we're seeing in the digital infra space is different pools of investors converging and looking at the same assets. We have certain investors that look for a certain stability and predictability of cash flows and that is reflective in the rates of return they require," Wallis says.

"But we have other investors that do take greater involvement in looking to actively manage these styles of companies and generate additional returns through a whole range of different business initiatives."

Different investors are looking at different business cases for the assets, depending on how comfortable they are in making assumptions about the asset's cashflow.

"The capital-intensive nature of these assets in terms of barriers for competition, the defensibility and predictability of associated cash flows and commercial arrangements and the fundamental drivers of underlying demand means there has been significant interest and involvement by some of the investors more traditionally focused on core infrastructure style assets," Wallis says.

"These assets have also generated interest from other investors with different return requirements and operating models — such as some of the more traditional private equity players."

The appeal to different types of



investors ultimately reflects the range of underlying different commercial arrangements, business models and structures across the digital infrastructure

landscape. In fact, in some instances, private equity and more traditional infrastructure investors have put funds into the same asset, but each with different underlying arrangements.

The growing interest in digital infrastructure investment comes after the COVID-19 pandemic increased demand for working and shopping from home and for businesses to digitise more of their processes.

While this increased demand for data and connectivity, Wallis says it was just an acceleration of trends which would have occurred anyway, but over a longer period.

However, the pandemic did demonstrate that digital assets can provide ongoing cashflows when other infrastructure assets — such as airports for instance — were affected by the pandemic.

"When you have a broader portfolio and a series of different investments and a series of different uncorrelated cashflows, you're getting diversity of cashflows that perform differently in different environments," he says.

Wallis says the upswing in interest for digital infrastructure assets comes amid the broader trend of investors seeking real assets, as the increasing amount of global savings leaves more capital looking for a home.

"It's not in the context of doing this instead of doing something else," Wallis says of investing in digital infrastructure. "This is one of many areas that are providing a series of cash flows within the right commercial arrangements where there are sufficient barriers of entry, there's sufficient predictability and there's defensibility around cash flow."

From previous page

## Businesses must bank on a secure future

have tens of thousands of servers, tens of thousands of computer systems, hundreds of branches, both in Australia and around the world. And so it's an incredibly complex exercise to ensure that we continue to lift the bar against an increasing threat."

Utilising part of Bugcrowd's army of 250,000 white hat hackers globally, the challenge for the elite hacker army is to find vulnerabilities in NAB's systems. As founder of Bugcrowd Casey Ellis points out, they act like bad guys but with good intentions.

Ellis compares cyber threats to a householder leaving their front door open — it invites criminals in and this "predates the internet by a couple of thousand years as a thing that people can exploit".

"With the digitisation of basically everything, we've also seen an acceleration of things that were pre-existing like open doors in terms of increasing human error and human fallibility. It creates the opportunity for an adversary to come in and exploit that as there's more houses and more streets.

## ■ Our adversaries are patient, very well organised and well-funded.

Patrick Wright, NAB

"The overall attack surface as a result of the internet is far larger than anything we've ever seen before. And I think it's accelerating quicker than we've really had time to keep up with, in order to try and keep it safe," Ellis says.

For Ellis, Bugcrowd was created to try and keep up with the rising threats by levelling the playing field with an army of good guy hackers.

"Our people all understand how to do security things with computers. We understand the different skills they all possess and we try to connect the right people with our customers' requirements."

In NAB's case, Bugcrowd found the right people to connect into their systems and provide the bank with the knowledge of where vulnerabilities might exist.

Ellis says this is just one of the things the company does with NAB but at its simplest level, the bank has set up a neighbourhood watch program for the internet where Bugcrowd's people identify potential security issues.

Having this army of hackers is something Australia needs as Hastie concedes we don't have enough people who are equipped to deal with the cyber security threat. We really need to start leaning into educating Australians about this, not just at university, but in the primary and secondary levels.

"There are going to be plenty of jobs in the future, whether it be in government or industry for Australians to serve in a cyber role of some form," Hastie says.

Wright says "there really can't be a digital economy without a robust cyber security ecosystem".

"The easiest thing to do is to turn off your digital world but that's not the future. We just need to think about security from the very get-go as we construct systems and ensure security elements are embedded in each layer of the tech ecosystem."

As for the future, Wright says "he's a glass half full guy".

"There a lot of great stuff happening around the world with law enforcement and government agencies. Our adversaries are patient, very well organised and well-funded, but I'm very hopeful that the work we're doing as Team Australia is making this an uncomfortable place for the cyber criminals to operate."

# Data-driven strategies will make a difference

## Structural shifts

Mark Eggleton

In an interview with *The Australian Financial Review* a few years ago, global data consultant and former Amazon chief data scientist Andreas Weigend commented that data provides all the answers but the challenge for organisations is asking the right questions.

Charlotte Cadness, NAB's executive digital data and insights for corporate and institutional banking, says asking the right questions is the next big step in the big data story.

As digitisation of the economy cuts across sectors and generations, Cadness says getting the questions right will see society move "beyond summary statistics and really get to insight".

She says NAB and its clients sometimes don't know what questions they want to ask, and it is the analysis of the collected data that informs the questions "so you can move beyond just information to insight".

In Australia over the past 18 months, data has come of age, informing government policies and helping businesses finetune their offerings, especially as they have pivoted during the pandemic.

Data has assisted Australia on its road to recovery and helped us cope with structural shifts as more people work from home. It has also helped business and government better understand how these shifts are playing out across the nation.

Importantly, it has helped society respond more quickly to change as we have had faster access to information and, armed with that information, been able to adjust quickly.

Cadness says NAB has shared its anonymised aggregated data with government, which has helped provide clarity around which segments of the economy have been the most affected by COVID-19.

"When we have emerged from lockdowns, we can see what the impact is within a couple of days and where people are spending their money," she says.

"While that's one aspect of data use, another is to help our larger business customers in particular navigate their way through what trends they've seen. What will help them understand what's the biggest bricks-and-mortar footprint for them and what does online spending look like?"

"They can use data to inform their strategic decisions and also see what the impact of those decisions is as well."



From summary to insight: NAB's Charlotte Cadness.

While the narrative around data capture and its use has been primarily positive coming out of the pandemic, we are starting to ask the larger hard questions associated with data collection and privacy.

Author and Harvard Business School Professor Emeritus Shoshana Zuboff says we live in the digital century during the formative years of the information civilisation.

"Our time is comparable to the early era of industrialisation, when owners had all the power, their property rights privileged above all other considerations," Zuboff says.

She says the danger is that companies can now "stake a claim to people's lives as free raw material for the extraction of behavioural data".

Writing in *The New York Times*

earlier this year, Zuboff suggested we live in a new era where the idea of our feelings being for sale is suddenly a reality. Humanity has never thought of feelings being for sale because they are inalienable, but now our fears or thoughts are considered fodder for an algorithm and are just "another data point in the trillions that are fed to the machines" every day.

According to Zuboff, the challenge for democracies is we now "have a democratic information civilisation to build, and there is no time to waste".

Cadness agrees much has to be done as we are on a journey to build out our digital future and we're still learning.

"Privacy laws have tried to be technology-neutral, but it can be hard for the law to keep pace with this fast-emerging technology," she says.

"The EU, for example, is proposing businesses like NAB spend a lot of time thinking about the responsibilities they have with people's data."

"At NAB, we have a data privacy and ethics team who we work very closely with so we better understand our role as custodians of the data and its intrinsic value. It's something we are very thoughtful about as are the wider business community."

As long as business and government continue to keep the importance of privacy and ethics top of mind, Cadness is positive about the future.

"We absolutely must keep businesses to account in terms of transparency and how we use data and if we get it right it's only going to benefit our customers, the community and society as whole," she says.





Democratisation of investing can empower retail investors to keep sustainability in view.

# Digitisation of finance shows the way to a better outcome

## Fractionalising assets

Christopher Niesche

The digitisation of finance is ushering in new asset classes and new opportunities for investors and helping to create a more efficient, inclusive and sustainable future.

Put simply, the digitisation of finance is the automation of the processes involved in financial and investment transactions, with the ultimate end-point that financial instruments become programmable, which creates new ways of investing.

Lisa Wade, director of product development at NAB, says technology will open up a wider range of asset classes to investors, particularly by fractionalising large assets, that is by digitally dividing the asset into thousands or millions of investable units.

She uses the example of a large skyscraper, an investment that would be out of reach for the average investor.

But it's possible to create a "digital twin" of the skyscraper, which holds all the paperwork that is associated with investing in the asset and all of the legal behind it embedded into a smart contract.

The resulting "token", which digitally represents the skyscraper, can then be divided into tiny pieces.

"It's the blurring of the line between public and private markets. Previously, public assets like bonds and equities were really what we could invest in, and now we'll be able to access private markets in the same way as we're able to access public markets," Wade says.

NAB hasn't started deploying the technology in real trades, but is preparing for its introduction with pilots and proof of concept projects.

Wade says the democratising of investing, as she calls it, can also facilitate more sustainable investing, by allowing retail investors to put funds into assets such as wind and solar generators.

"If I can fractionalise a wind farm then I can buy one one-millionth of the wind farm. Then all of a sudden I can really have a sustainable portfolio and have the impact that I want in the world," Wade says.

The digitisation of finance will also create large amounts of data that will have its own value, firstly in helping the data owners to make better



Dividing big assets will work for investors, says NAB's Lisa Wade.

investment decisions, but also as a saleable asset in its own right, to other investors wanting to gain insights.

Tokenisation will also change funds' asset allocations, by altering the risk profile on some assets.

**A large real asset might carry a significant amount of risk but if fractionalised it boosts liquidity.**

A large real asset might carry a significant amount of risk because of a lack of liquidity, but if the asset is then fractionalised it boosts liquidity.

"I'm shifting the underlying investment risk of that asset, therefore it will change the mix of my tactical and strategic asset allocation," Wade says.

Digitisation of finance draws on technologies including 5G, the Internet of Things, artificial intelligence and machine learning, but at its heart is distributed ledger technology and blockchain, which allow for programmable assets, which Wade describes as a "true game changer".

Programmable assets can "talk" to each other when settling a transaction. Wade provides a simple explanation: "The money says, 'You have to do five things for me to pay you'. The asset says to the money, 'I'm here. I'm doing all of those things.'"

"And then they work out that they've both done them and then the settlement happens."

Wade says the glue which holds the process together is a central bank digital currency, or CBDC, where a digital token would represent the virtual form of a fiat currency such as the Australian dollar.

These are similar in some respects to bitcoin or other crypto currencies, but importantly are issued by countries' central banks, such as the Reserve Bank of Australia (RBA).

Crucially, these currencies are programmable, so can facilitate automatic transactions and settlements.

Australia is investigating the issuance of its own CBDC, with the RBA having recently partnered with NAB, the Commonwealth Bank, Perpetual and blockchain technology company ConsenSys Software to explore the potential use and implications of a wholesale CBDC using distributed ledger technology.

The project involved the development of a proof-of-concept for the issuance of a tokenised CBDC that can be used by wholesale market participants for the funding, settlement and repayment of a tokenised syndicated loan.

Chris Thompson, deputy head of the RBA payments policy department, says the RBA is considering the use cases for a CBDC in the wake of this and other projects but can already see some potential benefits.

One is increasing speed and reducing settlement risk when both the tokenised currency and the asset are on the same blockchain.

"Because when you've got both the asset and the cash on the same platform, you can do atomic settlement, which means the cash and asset tokens are exchanged instantaneously, and in such a way as to ensure that the transfer of one token occurs if and only if the other transfers," he says.

He says programmable money can potentially reduce settlement risk by removing humans from the process.

But Thompson says any introduction of a CBDC is likely to be a long-term process.

"We see this as being part of a journey of a research program that we're doing on CBDC.

"This is going to play out probably over quite a number of years, so we're researching what are the use cases, what's the value add, what are the implications," he says.

# Industry insight

Comment by  
**David Gall**  
Group Executive Corporate  
and Institutional Banking  
National Australia Bank



This content is produced by The Australian Financial Review in commercial partnership with NAB.

When we examine how our economy has been transformed in recent years, we will look back on the last 12 months as a time when Australians became very adaptable, using innovation and digitisation in different ways to serve their customers over a crisis.

In March last year for example, NAB effectively moved its entire workforce of 34,000 people to remote working in a matter of weeks. This may not have been possible even a year or two earlier, but we were able to adopt new ways of working almost overnight.

Yet, we were far from the only Australian company to pivot and adopt digital ways of working during last year's crisis.

Right across the business community, organisations thought deeply about what their business models might look like in the future. They've used the pandemic to examine the potential of new markets as well as improving access to existing markets. What organisations also discovered were new ways to utilise technology to improve business efficiency.

One example is how local retailers found new markets by increasing their online sales and platforms. However, this wasn't confined to the retail sector.

We've got examples of businesses in planning and events or hospitality who have switched business models to online direct with significant increase in sales and the creation of new jobs.

Unemployment has remained low as new jobs have been created. Research undertaken by AlphaBeta Advisors and Data 61 estimates the potential benefits to the Australian economy through digitalisation to be as much as \$315 billion over the next decade, with the potential to create up to a quarter of a million new jobs by 2025.

Importantly, these new digital economy roles may be higher paying. With wage stagnation carefully monitored by the Reserve Bank, the creation of new jobs may stimulate wage growth.

They drive genuine productivity growth so you can afford to pay more rather than just driving the cost of wage rises into the economy.

Driving Australia forward in the digital economy doesn't just mean wholeheartedly embracing technology.



Shopping in Australian cities has adapted to pandemic conditions. PHOTO: GETTY

We have to use the momentum we've built over the last year to continue enacting broader structural change and stay on this trajectory.

This also means more investment in infrastructure critical to the country's future including stronger investment in digital assets such as a faster rollout of our 5G network and data centres to satisfy the huge demand for cloud services coming from business.

Our role as a bank is to provide funding to business and government to build the infrastructure Australia will need to thrive in a global digital economy.

At a federal and state level, we're not only supporting the construction of hard infrastructure such as rail and roads but digital infrastructure that supports data centres, mobile towers and even smart manufacturing.

We're also supporting new business opportunities and commercial models that open up the competitive landscape in electronic payments.

New players in the payments space are streamlining processes.

*Our role as a bank is to provide funding to business and government to build the infrastructure Australia will need to thrive in a global digital economy.*

We call it co-opetition with start-ups and fintechs that might actually partner with banks in various parts of the payments value chain and this is putting choice into the hands of consumers.

Beyond new opportunities in the digital space, there's plenty of scope for technology to broaden the appeal of industries where Australia already has a natural advantage.

The agriculture sector, for example, is beginning to think differently about how we can feed the fast-growing economies across the world.

We know our farmers are some of the most innovative in the world and now they're using technology to really build on our credentials as a safe, clean and green food source.

Indeed, while the opportunities appear boundless, consideration of the risks associated with the digital economy is also important.

We must continue to invest in cyber defences. NAB has a role to play here, in helping our clients understand and navigate the cyber threat landscape.

If we navigate the risks well, we approach a future with real optimism.

The last 12 months have again proven just how resilient and adaptable Australians are.

The challenge now is to build on this momentum by investing in the digital economy and creating productivity and real growth for our nation.



# Seamless payment systems heating up

## Transactions

Christopher Niesche

The most common way businesses interact with their customers is when the customer makes a payment, and so businesses need to make their payments as easy and as seamless as possible, says Shane Conway, an executive in transaction banking at National Australia Bank.

The increasing importance of payments is underscored by Reserve Bank data showing that Australians make on average 500 payments a year, up from 200 a decade ago.

At the same time, the way Australians pay is rapidly changing. Payments on the instant New Payments Platform and through debit cards – both in mobile wallets and tap-and-go – are the fastest-growing payment methods, with cash and cheques declining.

“What we’re seeing is businesses are having to really recognise those trends in how they set up their customer experience,” Conway says. “So making it easy to tap and go, putting the terminal in a prominent place so you can easily just tap your card; making sure if you’re an e-commerce site that you’ve got all the different – or at least a wide array of – ways to pay, whether it’s PayPal, debit card, credit card, some kind of buy now, pay later solution.”

For businesses, the easier they make it for their customers to pay, the more likely they will increase their sales.

Businesses are also taking advantage of the near-instantaneous payment capability of the New Payments Platform (NPP).

Small businesses are optimising working capital by paying later and receiving instantaneous payments, while larger businesses are also optimising liquidity and driving efficiency by automating as much of the payments process as possible.

## ■ What we’re seeing is a stronger mindset of let’s collaborate with fintechs.

Shane Conway, NAB

As payments have grown more important, banks have started collaborating with fintechs to build payment solutions to customers. In fact, about 100 of Australia’s 700 fintechs are payments-focused.

“If you went back five, six, seven years ago, the dominant narrative at the time was that fintechs were going to take over the world and banks would be irrelevant. What we’re seeing now is a much stronger mindset of let’s collab-



Athena co-founders Michael Starkey and Nathan Walsh. PHOTO: RHETT WYMAN

orate with fintechs to offer businesses innovative solutions,” Conway says.

“Our view is banks can’t do everything, and they certainly can’t do it as quickly as some fintechs, but the customer need is quite urgent. So we’re happy to collaborate where we think we can solve a customer problem.”

Fintechs usually offer only the one product, so they bring a sharp focus on just one customer problem and can get a solution to market more quickly.

Banks bring to the collaboration access to the instant payment rails – the NPP – and expertise.

In the same way that a traditional banker will get to know a business and advise it on, for instance, how to structure a loan, banks are trying to understand the payment needs of individual

clients and helping them solve a payments problem.

Home loan provider Athena is currently collaborating with NAB to build an instant payment solution for its customers. As a specialist home loan provider, Athena focuses solely on home loans and doesn’t provide other banking services such as transaction accounts or credit cards.

It is currently working on developing a solution to allow its customers to transfer money from their Athena redraw facility into their transaction accounts when they need to go shopping or pay a bill.

“So if you think about having money in a redraw account and then you want to actually go shopping and you need to access \$50 out of your redraw account,

you will shortly be able to do that within seconds by basically effecting a new payments platform payment over to your bank,” Michael Starkey, co-founder of Athena, says.

For Athena, it’s a chance to provide its customers with better and richer functionality via an improved payments proposition and to continue to specialise in what it does best.

“For a fintech like Athena, it allows us to be a specialist mortgage player and not have to worry too much about being a bank, for example, and opening and having all transactions and credit cards and all that sort of thing, because customers can do all that elsewhere,” Starkey says.

Using the NPP’s PayID function – where customers can use an identifier such as an email address or mobile phone number instead of a bank account number – is important for customers to be sure they’re paying the right person, Starkey says.

There is a central role for banks in providing security and stability in payments when they develop solutions for customers, despite the flourishing of payment-focused fintechs, NAB’s Conway says.

“The role of banks will be to partner with those firms so that you’re giving your customers the best possible experience and the best possible solutions for their problems,” Conway says.

“The banks perform the role that they’re really good at, which is protecting people’s identity, protecting people’s money, protecting the system overall and making it a stable system so that people have high confidence that payments are going to be made and received and settled without issue or error,” he says.

more  
than  
money



# AUSTRALIA’S TECH FUTURE NEEDS FUNDING TODAY

We’re helping Australia’s technology pioneers keep moving forward. That’s why we committed \$2 billion to funding emerging tech over five years,\* backing them with the support they need as they grow and scale.

Our Corporate & Institutional team can help with your big idea.

🔍 NAB Big Ideas

\*From June 2019 to May 2024

© 2021 National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686. A163474-0521A