


# Online Payments – The Future of the Australian Economy

Nigel Phair  
March 2021



This report is submitted by  
UNSW Canberra Cyber

**For further information:**

Nigel Phair: [n.phair@adfa.edu.au](mailto:n.phair@adfa.edu.au)

Director, UNSW Canberra Cyber  
Ground Floor, Building 13  
Northcott Dr, Campbell ACT 2612  
UNSW Canberra ACT 2600  
Australia  
T + 61 2 626 88501  
[unsw.adfa.edu.au](http://unsw.adfa.edu.au)

The legal entity for the contract is the University of New South Wales  
ABN: 57 195 873 179  
The UNSW is a GST-registered organisation. CRICOS Provider Code 00098G

This report was commissioned by Mastercard

# Contents

<b>Contents</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>The Internet and the Australian Economy</b>	<b>2</b>
<b>Online Payments</b>	<b>3</b>
<b>COVID-19 – accelerating changes in payments behaviour</b>	<b>4</b>
<b>Payment card fraud is on the decline</b>	<b>5</b>
<b>Building trust and safety online</b>	<b>5</b>
<b>Australia leads the way in payments innovation</b>	<b>6</b>
<b>Conclusion</b>	<b>8</b>

# Introduction

Australians love technology and enjoy using it to make safe, secure and convenient online transactions. Developments in technology, new entrants and innovation in payments have altered the retail payments landscape. This is a good thing for businesses and consumers, however as much as we embrace innovation, the non-negotiable element which will drive adoption – and therefore economic growth – is customer trust and safety. With 97% of Australian businesses employing less than 20 staff and having to manage competing business priorities with limited resources, it's convenient to push online security to one side. Australian businesses require specific advice and a holistic approach to better defend themselves from cyber security threats.

Online payments have increased during COVID-19 and will continue to drive prosperity in our economy. Ensuring appropriate robust security is built into the payments ecosystem will be the key to success.

## The Internet and the Australian Economy

Our lives have fundamentally changed. Over time, we have moved from video rentals to Netflix and from taxis to Uber. This innovation has been underpinned by secure online transactions.

Internet-based technology has fundamentally changed the make-up of the Australian economy. It has opened up global opportunities and reduced barriers to going to market. It has also opened up innovation in payments.

Over the past 20 years internet usage and penetration has rapidly increased – globally in 2000 there were 304m users, representing just 5% of the population. In early 2020 there were 4,574m users, representing nearly 60% of the global population.<sup>1</sup>

In Australia in 2000, there were 6.6m internet users representing nearly 34% of the population.<sup>2</sup> This increased to almost 22.3m users in 2020 - around 88% of the population.<sup>3</sup> 86% of Australian households are connected to the internet – and 80% of Australians are online daily<sup>4</sup> – principally via desktop/laptops, mobile smart devices and TV, music/video players. Since the beginning of COVID-19, household peak download throughput has increased by 25 percent.<sup>5</sup> More than 95% of Australian businesses have internet connectivity, with over half having a web site, social media presence and making and accepting payments online.<sup>6</sup>

Online retail sales are now equivalent to approximately 9% of traditional retail sales as Australia catches up to other more mature online markets such as the USA, China and United Kingdom where online retail sales market penetration is greater than 15% of total retail sales.<sup>7</sup>

---

<sup>1</sup> Internet World Stats. *Internet Growth Statistics* [<https://www.internetworldstats.com/emarketing.htm>]

<sup>2</sup> Ibid.

<sup>3</sup> We Are Social. *Digital 2020 in Australia*. [<https://wearesocial.com/au/blog/2020/02/digital-2020-in-australia-analysis>]

<sup>4</sup> Department of Home Affairs. *Australia's Cyber Security Strategy*. [<https://cybersecuritystrategy.homeaffairs.gov.au>]

<sup>5</sup> CRN. *NBN reveals extent of data surge during virus crisis* [<https://www.crn.com.au/news/nbn-reveals-extent-of-data-surge-during-virus-crisis-545958>]

<sup>6</sup> Australian Bureau of Statistics. *Summary of IT Use and Innovation in Australian Business, 2016-17*. [<https://www.abs.gov.au/ausstats/abs@.nsf/mf/8166.0>]

<sup>7</sup> McGrathNicol. *IN RETAIL: COVID-19 special edition #1*. [<https://www.mcgrathnicol.com/insight/in-retail-covid-19-special-edition-1/>]

# Online Payments

Online payments are a massive enabler for the economy. They have facilitated significant innovation which consumers are keen to embrace. Consumers want to be able to transact online, often via mobile devices, yet need to have the confidence in the financial transaction process and that their personal and payment data will be secure.

Internet-based processing of commercial transactions allows a vendor to accept payments from a wider range of customers, greatly expanding the reach of a business and the ability to make sales beyond our shores. This is particularly important for small businesses during the COVID-19 pandemic, where opportunities for in-person transactions have decreased dramatically.

Small business and family enterprise in Australia, classified as businesses with less than 20 employees, account for almost 98% of businesses. The sector is growing fast and as such, presents many opportunities – and challenges – for those who dedicate themselves to pursuing a small business venture.<sup>8</sup>

97% of small businesses are connected to the internet, whilst 67% placed orders online and 44% received orders online. 91% of these businesses conduct online banking. This has resulted in small businesses being the target of 43% of all cybercrimes and that number is increasing. These attacks affect productivity, disrupt business activities, and cause loss of revenue. 53% of small businesses identify hacking as a major concern, with 89% having at least some concern about hacking.<sup>9</sup>

Given that many people now carry little or no cash, the reliability of electronic payment services has become critical to the smooth functioning of our economy.<sup>10</sup>

In November 2019, the New Payments Platform (NPP) processed an average of 1.1 million payments each day, worth about \$1.1 billion. The rate of take-up of fast retail payments in Australia is a little quicker than that in most other countries which have also introduced fast payments.<sup>11</sup> Online payments reduce cash use – measured as a proportion of sales, the cost of a cash transaction is around 2.5% – removing an unwanted (and costly) burden for businesses, while also decreasing the risk of COVID-19 transmission.<sup>12</sup>

Online payments also reduce the black economy. The black economy refers to people who operate entirely outside the tax and regulatory system or who are known to the authorities but do not correctly report their tax obligations. It encompasses a wide range of practices, including the payment and acceptance of cash off-the-books. The Australian Government introduced the *Currency (Restrictions on the Use of Cash) Bill 2019* in late 2019. The Bill gives effect to an economy-wide cash payment limit. The payments industry can help the Government achieve its broader aims in this regard via its innovation.

---

<sup>8</sup> Australian Small Business and Family Enterprise Ombudsman. *Small Business Counts. Small business in the Australian economy - July 2019* [<https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-small-business-counts2019.pdf>]

<sup>9</sup> Ibid

<sup>10</sup> Lowe, P. *A Payments System for the Digital Economy*. [<https://www.rba.gov.au/speeches/2019/sp-gov-2019-12-10.html>]

<sup>11</sup> Ibid

<sup>12</sup> Phair, N. *The Truth about Contactless Payments*. March 2016

## COVID-19 – accelerating changes in payments behaviour

During the COVID-19 pandemic, most businesses are focused on their ability to continue operating and, if so, what changes can be made to their business operations to accommodate the new working environment. This might include changing from in-person to online interaction with customers or examining the way employees can continue to work remotely from their home.

COVID-19 has also fundamentally changed many of our habits, including driving greater online payments. People are coming to terms with the realities of our interconnected world and what this means for work, social interaction and buying habits.

Reporting indicates significant changes in financial behaviours and patterns in light of COVID-19. Many bank branches were closed due to public health and “lockdown” measures. Customers are therefore carrying out more transactions online. Certain population segments (e.g., the elderly, low-income groups, and remote or indigenous communities) may be less familiar with using online banking and e-commerce platforms, and therefore more susceptible to fraud. Data shows that online banking fraud targeting financial or account information is on the rise.<sup>13</sup>

In Australia, there are more than half a million customers (many aged over 70 years) who actively use a passbook account with no linked debit card. COVID-19 has prevented these account holders from participating in the banking system. To address this, the broader banking industry fast-tracked the provision of debit cards to this cohort. While this is a good idea, these customers may be more susceptible to online fraud.

Buying online during this time of uncertainty makes sense. The likelihood of an infected person contaminating commercial goods is low and the risk of catching COVID-19 from a package that has been moved, travelled, and exposed to different conditions and temperatures is also low.<sup>14</sup> Shopping habits are also changing, with fashion, apparel and luxury retailers having declining revenue; other industries, like grocery and food and beverage, have seen an unprecedented spike in demand.<sup>15</sup>

Additionally, as many stores begin to re-open many consumers may be reluctant to visit busy locations due to lingering concerns around their health. By this stage consumers will have become accustomed to buying most of their purchases online. When they are ready to spend again, it will start online – and more transactions are likely to stay online. Activity will return to shopping malls but digital will play a much larger role. Retailers with truly omni-channel experiences will be best positioned to benefit during the early recovery period.<sup>16</sup>

This change has also provided a new market for online criminals. Cybercriminals are pivoting their online criminal methods to take advantage of the COVID-19 pandemic. They continue to rapidly adapt their techniques in response to changes in the current environment. For example, malicious cyber adversaries are using COVID-19 themed phishing campaigns to obtain user credentials, allowing them to bypass security controls in order to gain access to accounts and networks belonging to individuals and businesses. This could include targeting employees working from home and the remote systems they are relying upon.<sup>17</sup>

---

<sup>13</sup> Financial Action Task Force. *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*. [<http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>]

<sup>14</sup> World Health Organisation. *Q&A on coronaviruses (COVID-19)*. [<https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses>]

<sup>15</sup> Antavo. *Comprehensive guide for grocery and food & beverage loyalty programs*. [<https://antavo.com/blog/grocery-food-beverages-loyalty-program>]

<sup>16</sup> KPMG. *COVID-19: Retail's survival and revival*. [<https://home.kpmg/au/en/home/insights/2020/04/coronavirus-covid-19-retail-survival-and-revival.html>]

<sup>17</sup> ACSC. *Threat update: COVID-19 malicious cyber activity*. [<https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020>]

## Payment card fraud is on the decline

Interestingly, payment card fraud has declined as spending by card has increased (not accounting for COVID-19).

Over \$819 billion was transacted on Australian cards in 2019, an increase of 3.9% on the prior year. Fraud accounted for 0.057% of that total, down from 0.073% in 2018.<sup>18</sup>

Physical card fraud, such as card counterfeit/skimming fraud, has also fallen by 15% to a record low of \$16.8 million. This is the result of the introductions of EMV chips on all Australian cards. This innovation is virtually impossible to reproduce by fraudsters and has effectively driven card present fraud in Australia to global record lows.

Internet e-commerce transactions are susceptible to card-not-present (CNP) fraud, which occurs when valid card details are stolen and then used to make purchases or other payments without the card, for example via online or by phone. This accounts for around 87% of all Australian card fraud.

CNP transactions in Australia grew by 16% in 2019 to \$220 billion. Over the same period, CNP fraud on Australian cards dropped by almost 18% to \$403 million – representing less than 0.2% of transactions.<sup>19</sup>

This decrease in total card fraud has been enabled by a number of initiatives, including the introduction of:<sup>20</sup>

- CNP Fraud Mitigation Framework – which defines the minimum requirement for an issuer and merchant (or acquirer or payment gateway) to authenticate CNP transactions, and mandates strong customer authentication for those issuers and merchants whose fraud rate is consistently in breach of agreed industry thresholds.
- Collaboration with the Joint Cyber Security Centre to identify ways in which the industry and Government can share actionable information on cyber security.
- EMV chip technology – Chip and PIN has been mandated in Australia at point-of-sale since 2014.
- 3D Secure – allowing consumers to authenticate themselves to their card issuer during remote purchases.
- Tokenisation – the process of replacing the 16-digit Personal Account Number on a card with a unique digital identifier (a token).

## Building trust and safety online

For companies that accept online payments, a breach of confidential customer data is among the most serious risks they face. Failure to protect data leads to financial costs, customer defections, loss of reputation and possible sanction, depending on the jurisdiction.

Yet while 80% of Australian small and medium businesses rate cyber security as important for their business, around half spend less than \$500 per year on this function. It is troubling that half of small

---

<sup>18</sup> Australian Payments Network. *Australian Payment Card Fraud 2020*.  
[[https://www.auspaynet.com.au/sites/default/files/2020-08/Fraud\\_Report\\_2020.pdf](https://www.auspaynet.com.au/sites/default/files/2020-08/Fraud_Report_2020.pdf)]

<sup>19</sup> Ibid

<sup>20</sup> Ibid

and medium businesses rate their cyber security understanding as 'average' and 20% do not know what phishing is.<sup>21</sup>

A key component of improving security, while not negatively impacting on customer experience, is payment card tokenisation, where the customer's primary account number (16-digit card number) is replaced with a series of randomly generated numbers in a 'token'. These tokens can then be passed through the internet to process the payment without actual bank details being exposed. Even if there is a data compromise of merchant systems, the information cannot be misused. Considering the low maturity of Australian small and medium-sized businesses, attempting the introduction of third-party tokens will not likely succeed due to the businesses inability to fund or execute.

The card schemes offer tokenisation services, based on the EMV payment token specification. Payment tokens provide merchants with an additional layer of security which works seamlessly in the background and when using a card schemes own proprietary tokens this enhances their other security measures. It provides peace of mind and a better experience to consumers, particularly for higher risk transactions.

Many solutions look for fraudulent purchases but regularly miss the key threat vector – where accounts are tested by mass-scale attacks. These attacks are becoming more sophisticated and impactful. These business-threatening attacks happen well before the account takeover occurs days, weeks or even months before you see a fraudulent transaction.<sup>22</sup>

The 3DS 2.0 protocol provides enhancements on the original version, including an ability to share greater data with a Merchant to inform a more assured risk-based decision. 3DS 2.0 is an advanced solution to make online payments simpler and safer, any time, across all devices. The solution evaluates every online payment in real time and either instantly approves and verifies the cardholder's identity for an additional layer of security.<sup>23</sup>

Should chargebacks be required, merchants need to be able to react in real time. For example, Ethoca's collaboration-based network, provides exclusive access to cardholder-confirmed fraud data that comes direct from a global network of card issuers. Because the alerts are confirmed fraud, a Merchant can act quickly to stop the fraud, refund the transaction and eliminate the chargeback.<sup>24</sup>

## Australia leads the way in payments innovation

The payments industry has a strong track record of innovation, including tools for businesses, consumer adoption and security measures. This has included everything from Chip and Pin, contactless payments, digital wallets and tokenisation.

Transactions that use card credentials stored electronically on mobile devices are becoming more popular. It is likely more card issuers in Australia will support the use of their cards in third-party digital wallets like Apple Pay. Wearable payment devices – including smart watches, rings and bracelets – have further expanded the range of devices through which card payments can be initiated. The uptake of these new payment options may reflect the additional functionality, convenience and/or security they offer relative to physical plastic cards.<sup>25</sup>

---

<sup>21</sup> Australian Signals Directorate. *Cyber Security and Australian Small Businesses*.  
[<https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf>]

<sup>22</sup> NuData Security. *Account takeover – The tip of the cyberthreat iceberg*.

<sup>23</sup> Mastercard. *Convenient and Secure Online Transactions: 3DS 2.0*

<sup>24</sup> Ethoca. *Ethoca Alerts*. [[www.ethoca.com](http://www.ethoca.com)]

<sup>25</sup> Reserve Bank of Australia. *Retail Payments Regulation and Policy Issues*.

[<https://www.rba.gov.au/publications/annual-reports/psb/2019/retail-payments-regulation-and-policy-issues.html>]  
UNSW Canberra | Cyber



This innovation extends to the development of security features through ‘security-by-design’ - the concept of taking a more proactive approach to payment security, baking security into a merchant’s payment infrastructure and not simply relying on reactive third-party security tools. For example, aftermarket tools run the risk of taking a reactive approach to cyber security, implementing measures only after an attack within a payment system has occurred, rather than building security into new products and services based on prior business risk calculations and new innovations.

This holistic approach is similar to the security differences between Apple’s iOS and the Android operating system. There is a far higher percentage of mobile malware targeting Android than iOS. Apple adopts a ‘walled garden’ approach – an enclosed environment which controls a user’s access to non-trusted apps therefore preventing access to malicious activity – using internal tools to vet all apps to avoid allowing malware through. It also has a better system when pushing upgrades to their operating system.<sup>26</sup>

The payment card industry has, over time, created a set of tools which automate the fundamental architecture of security within a payment process and a similar ‘walled garden’ approach by focusing on:<sup>27</sup>

1. Monitoring the behavioural interactions of the consumer and account accessing the payment ecosystem;
2. Reviewing the customers shopping cart, their payment credentials and verifying their identity;
3. Scoring fraud risk based on AI models; and
4. Managing any disputes.

The Government should ensure regulatory settings for the payments sector support continuous investment in innovation and security. Having the right regulatory framework, such as ISP codes of practice, helps Australia tap into emerging technologies, provides innovative businesses the ability to perform online transactions with customers, and protects consumers and the community. A one-size fits all regulatory approach does not work in the dynamic online payments industry – governments, industry, business and the community need to work together to identify the right tools and approaches to address the specific risks, issues and challenges of regulating new technologies.

When setting regulation, the Government should strive for businesses to reduce their exposure to cybercrime based on lessons learned from other nations, identification of current and emerging threats and the introduction of innovative security technologies. They should also encourage businesses to manage risk by enhancing their resilience, which enables the organisation to absorb the adverse impact of a security incident and re-establish itself quickly.

Proprietary fraud detection products and services, housed within an ecosystem, offer a better user experience, enhanced security controls and cheaper offerings, resulting in better financial and operational outcomes for Australian retailers. For example, tokenisation should only be assessed on security standards, not on any implications for product competition in the payments system. Token interoperability does not provide best practice security outcomes. The creation of a generic system of tokenisation carries “a significant cost burden, with the potential for these costs to ultimately be passed through to retailers in the form of higher card transaction costs.”<sup>28</sup>

The use of generic tokens is akin to a turnstile, providing a security control at the time the transaction commences, but not protecting the whole transaction ecosystem. A ‘walled-garden’ approach where the card scheme stacks all the security components together means they have more touch points of tactical information to make better strategic security decisions. It allows them to determine where fraud

---

<sup>26</sup> Norton. *Android vs iOS: Which is more secure?* [<https://au.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html>]

<sup>27</sup> MasterCard. *Security by design throughout the customer journey.*

<sup>28</sup> COSBOA. *Review of Retail Payments Regulation – Issues Paper.* [<https://www.rba.gov.au/payments-and-infrastructure/submissions/review-of-retail-payments-regulation/council-of-small-business-organisations.pdf>]

originates, pre, during and post transaction. Without the need to have multiple vendors, security data analytics provides more connected intelligence.

Fraud detection works best when security is baked into the transaction process, not bolted on by a third party later. This also reduces friction in the transaction, providing a safer and quicker payment. The payments industry is supporting Australian businesses of all sizes with cost-effective security solutions so they can safely and securely receive online payments.

## Conclusion

Global spending on cyber security is expected to almost double from around US\$126 billion in 2016 to US\$251 billion by 2026,<sup>29</sup> reflecting both the increased number of transactions and the growing sophistication of fraud. Australian merchants need to understand that while there are many benefits to being online, there is also a potential downside they need to mitigate.

Just like a traditional 'bricks and mortar' business invests in physical controls, such as locks on doors and security cameras, an online business likewise needs to undertake due diligence in risk-managing their internet-based transactions.

Whilst there are productivity savings to be made through the introduction of technology, there is a cost incurred by implementing security. However, the return on investment of security spend is compelling when considering the small cost-per-transaction, a safer customer experience, lower insurance premiums and the ongoing viability of businesses.

The best security is the security you don't "see." For example, many public spaces now have large planter boxes evenly spaced at road junctions. These are not there as an aesthetic feature, rather they are to stop any vehicle-based crime. To the pedestrian this is a smooth experience, keeping them at ease, whilst not being an overt sign of any potential problem. This is a prime example of security-by-design.

We should adopt a similar philosophy with online payment security. Intelligence-led solutions, monitoring transactions for behavioural characteristics, reviewed for identity purposes and scored on a risk basis is critical to keeping payments safe.

---

<sup>29</sup> AustCyber. *Australia's Cyber Security Sector Competitiveness Plan 2017*. [<https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2017>]



## UNSW Canberra

Northcott Drive  
Canberra, ACT 2600

[cyber@adfa.edu.au](mailto:cyber@adfa.edu.au)  
[unsw.adfa.edu.au/cyber](http://unsw.adfa.edu.au/cyber)

CRICOS No. 00098G