accentureconsulting

SECURE CARDS

AS PAYMENT FRAUD CLIMBS, TIME FOR NEW SOLUTIONS

Card fraud continues to climb, with Card Not Present (CNP) fraud involving Australian-issued cards accounting for 85 percent of the crime, or nearly half a billion dollars.[1]

The burden of CNP fraud—predominantly carried out via online transactions—falls on card-holders and merchants, although it is the issuing banks that are best-placed to combat it via a range of technological solutions.

Among those solutions is Motion Code, in which the card's CVV code changes every hour—vastly reducing the scope for fraud.

In order to work best, any solution looking to tackle fraud must also preserve the customer experience.

Banks should consider technological solutions not only to shrink fraud and associated costs, but to rebuild their reputations in the wake of the Royal Commission hearings.

1. AN ISSUE BOTH LOCAL AND GLOBAL

Fraud on Australian-issued cards is a growing and costly problem: in the year to June 2018 it totalled A$551 million (excluding fraud on proprietary debit cards[2]) on transactions worth A$767 billion. That was up nearly 5 percent on the previous 12-month period.[3]

Anti-fraud measures such as chip-and-PIN have helped in tackling the problem of counterfeit cards being used with ATMs and in-store. The result is that fraudsters have taken their trade into the e-commerce space, as the Australian Payments Network (AusPayNet), the payments industry's self-regulatory body, highlighted in its latest fraud report: "As chip technology provides strong protection against counterfeit cards, fraud continues to migrate to online channels."[4]

AusPayNet's data shows that by far the biggest problem is Card Not Present (CNP) fraud, which occurs when criminals use valid cards whose details have been stolen in order to buy goods or services online. CNP fraud on Australian-issued cards totalled A$478 million in the 12 months to June 2018 (see chart), split roughly equally between fraud committed abroad and at home. As a category, CNP fraud comprised 85 percent of the total value of card fraud on Australian-issued cards, up nearly 8 percent on the previous 12-month period.[5]

Scheme credit, debit and charge card fraud perpetrated in Australia and overseas on Australian-issued cards

1 July 2017 – 30 June 2018

CATEGORY	IN AUSTRALIA		OVERSEAS		TOTAL	
	Transactions	Value ($)	Transactions	Value ($)	Transactions	Value ($)
Lost / Stolen	371,005	31,597,872	78,357	15,898,186	449,362	47,478,058
Never Received	34,180	5,831,341	2,059	399,968	36,239	6,231,308
Fradulent Application	6,795	1,747,602	2,039	646,300	8,834	2,393,902
Counterfeit / Skimming	19,135	4,660,079	39,796	10,275,330	58,931	14,935,409
Card Not Present (CNP)	1,808,022	249,226,028	1,562,242	228,694,673	3,370,264	477,920,701
Other	3,865	919,273	3,887	891,817	7,752	1,811,091
Total	**2,243,002**	**293,964,195**	**1,688,380**	**256,806,274**	**3,931,382**	**550,770,470**

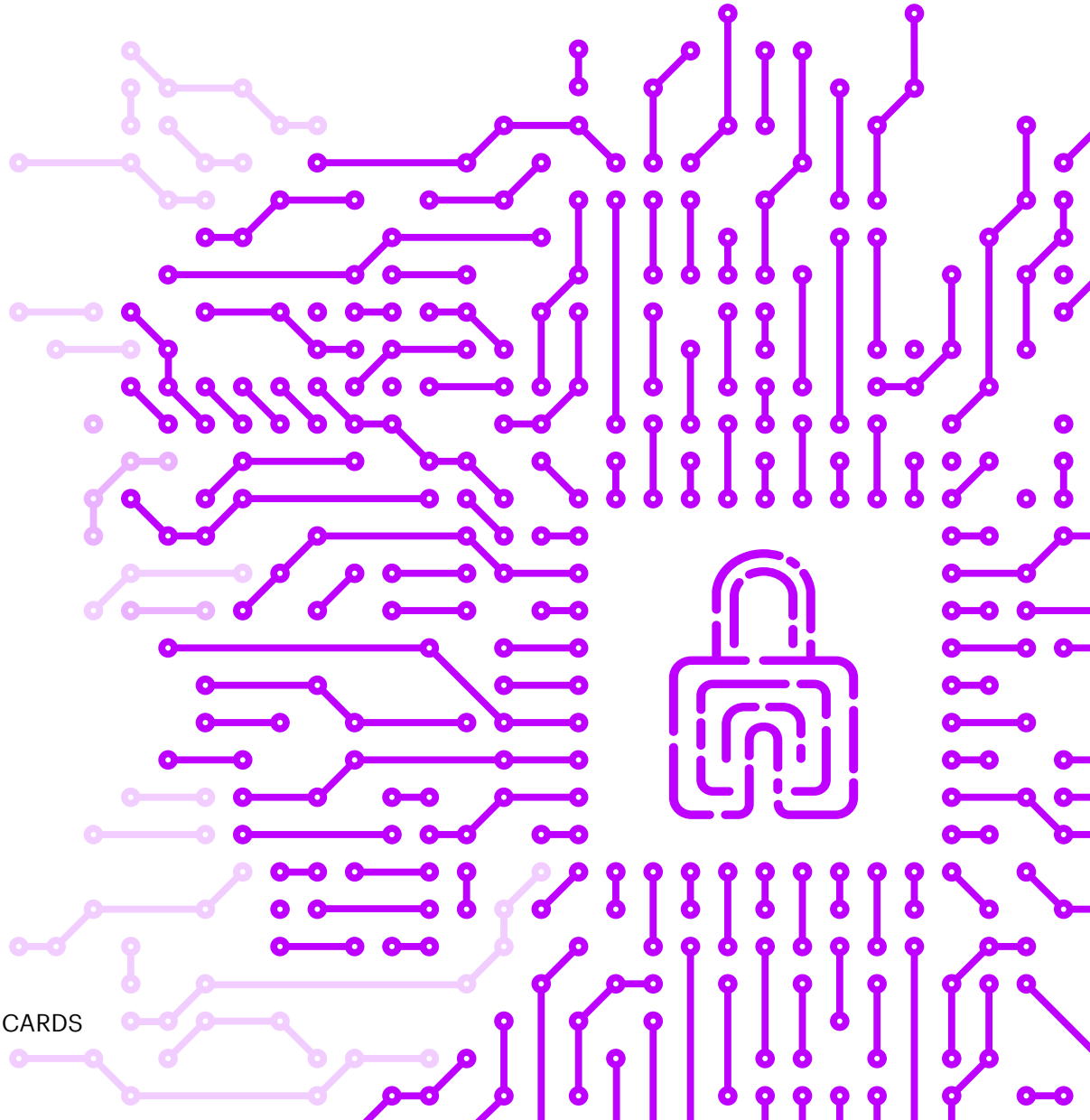
Note: The number of fraud transactions does not represent the number of cards or consumers affected. Typically, multiple fraud transactions are made on a single card.

Source: Australian Payments Network

Globally, CNP fraud is thought to cost between US$25-40 billion annually.[6] Recent research predicts it will cost retailers around the world US$130 billion between 2018-2023, with the growth in CNP fraud globally likely to average 14 percent a year.[7] The reasons for the rise, the researchers said, were retailer inertia in using measures to combat fraud coupled with more complex approaches to the crime by fraudsters.

It is likely to climb in APAC too: analytics firm FICO said recently nearly three-quarters of APAC banks expect CNP fraud will rise this year, and listed it as one of their two key challenges (along with application fraud).[8]

The good news is that, although card fraud overall has grown in Australia, its rate of increase has slowed thanks to a range of measures to combat it: card fraud was up 5 percent in calendar year 2017, but that was a far slower increase than seen in 2016 (up 16 percent) and 2015 (up 19 percent).[9] In other words, taking preventative and proactive measures does work, and those work particularly well when they preserve the customer experience.



2. CARD FRAUD ARMS RACE

CNP fraud dominates simply because online purchases require only the details printed or embossed on the physical card—not the card itself. That allows anyone with these details effectively to make a purchase.

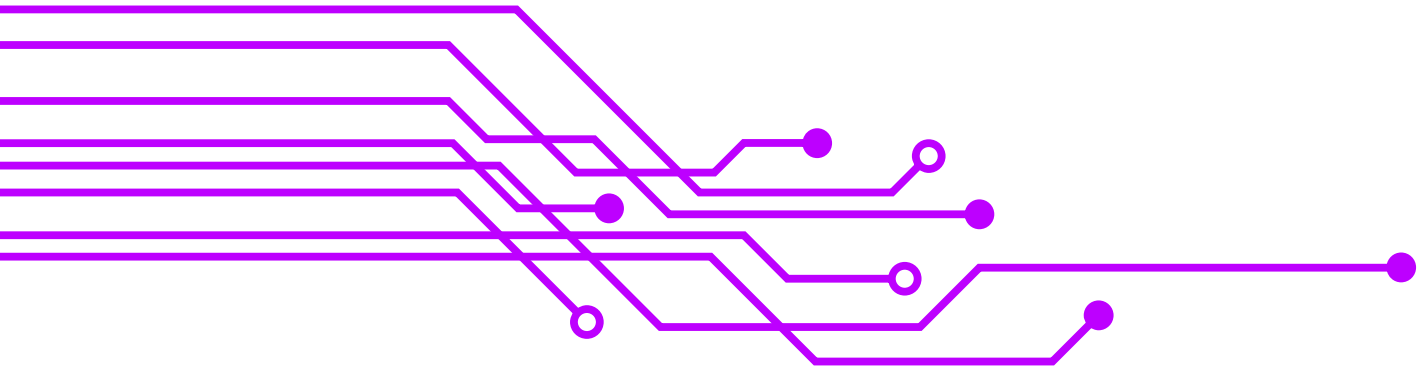
The internet has enabled criminals in other ways too, allowing them to sell card details on the dark web, and to receive payment in anonymous cryptocurrencies.

Over the past two decades, combating card fraud has been a constant arms race, with criminals finding and exploiting loopholes, which are then closed, before they seek out and exploit others. As a result of this constant battle, a range of mitigating technologies has been developed that can significantly cut fraud.

The advent of chip-and-PIN in the 2000s, for instance, made a significant impact on card-present fraud. In the UK, losses dropped 13 percent in its first year of use[10] while in Australia, similar initiatives to combat skimming saw the cost of that crime nearly halve to reach a record low of A$23 million in the 12 months to June 2018.[11]

This new age of solutions provides a win-win for banks, merchants, card schemes and consumers. The benefits for acting aren't just financial: fraud has other costs, including social and reputational damage, as well as the time it takes for parties to deal with each fraud. Combating fraud lowers costs, increases trust between consumers and banks, bolsters e-commerce, and—not insignificantly for Australian banks in the wake of the Royal Commission's findings—can help to improve reputations.

Taking action, therefore, constitutes good business sense for banks, but success requires them to reimagine the role of identity in securing digital payments and to understand which solutions are best-placed to achieve that.



CASH NO LONGER KING

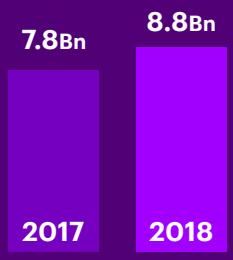
As the Reserve Bank of Australia recently noted, consumers worldwide are increasingly using cards and mobile payments rather than cash.

Australians are well ahead on that trend, with card use up nearly 13 percent in 2018 alone (see chart). This shift has been helped by the arrival of contactless payments, which has paved the way for using cards over cash, even for small-value payments.

Globally, Australians are far ahead of many countries when it comes to card payments,[12] with cards comfortably outstripping cash in 2016 by 52 percent to 37 percent as the preferred way to pay, according to the Reserve Bank of Australia,[13] cementing a seemingly unstoppable trend.

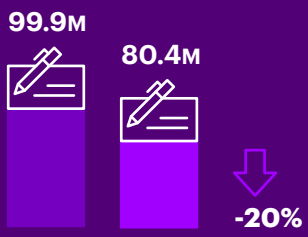
The downside of this move away from cash and towards digital payments is, as we have seen, a far greater scope for fraud.

Consumers are consistently choosing digital payment methods



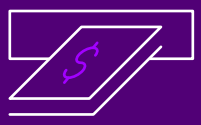
CARD USE GREW BY A RECORD 12.7%

DIRECT ENTRY PAYMENTS GREW BY 4.2% TO 3.9 BILLION



CHEQUE USE CONTINUES TO PLUMMET

ATM WITHDRAWALS DROPPED TO 600 MILLION



DOWN 4%

Source: Reserve Bank of Australia

Source: "The rise of digital payments," Australian Payments Network Annual Review 2018.

3. OPEN SESAME: AUGMENTING THE CARDHOLDER'S IDENTITY

Provided they have taken due care, Australian consumers are not liable for fraud; that responsibility typically lies with the merchants accepting the payment.

Stripe, a U.S.-based online payments technology firm, noted in its 2017 report that it costs merchants dearly: every dollar of a fraudulent transaction costs online stores another US$2.62 in associated costs on average.

Stripe also found that repeat fraud on compromised cards is common, with more than 40 percent of such cards being used for two or more fraudulent transactions.[14] In Australia, too, fraudsters typically make multiple transactions on each card.[15]

Banks incur expenses too: the cost of servicing a chargeback is typically in the AUD$70-100 range, which means that in practice banks often don't challenge disputed payments below AUD$100.

The lucrative nature of card fraud combined with the increased use of cards over cash means criminals are industrialising their capabilities, carrying out fraud and attacks on a much larger scale than before.

This range of crimes, which has morphed in recent years, requires a range of solutions —something AusPayNet recently noted. It said combatting CNP fraud in e-commerce was "a key priority", particularly given the success of chip technology in cutting fraud in other areas.[16]

For their part, banks are examining multifactor authentication (MFA) solutions including tokens provided by mobile phone, one-time passwords and biometrics.

It remains the case that the best way to combat fraud is not just to prevent it, but to deter it up front, and in this, banks must be much more proactive, actively working to prevent the crime rather than simply limiting the losses associated with it. If criminals know they have a small window of opportunity from the time that they steal someone's card details to committing fraud with that card —or, more likely, selling those details on the dark web—they are less likely to do so.

At the same time, measures to prevent fraud must preserve the customer experience. The example of 3DS, also known as 3D-Secure, is instructive. 3DS, which consumers know by the names 'Verified by Visa' and 'Mastercard Secure Code', adds an extra layer of security for online transactions. However, the original version provided a clunky redirect experience, with the cardholder having to remember password information in order to have their purchase processed. The result: 20 percent of authentications failed, and as many as one in seven online shopping carts were abandoned on checkout.[17] In turn, many merchants dropped 3DS as a solution.

Successful solutions to prevent fraud, then, must not only augment or support the cardholder's identity; they must not detract from the customer experience or cause shoppers to abandon their purchases by adding friction to the process.

MOTION CODE

One innovative, frictionless solution is Motion Code.

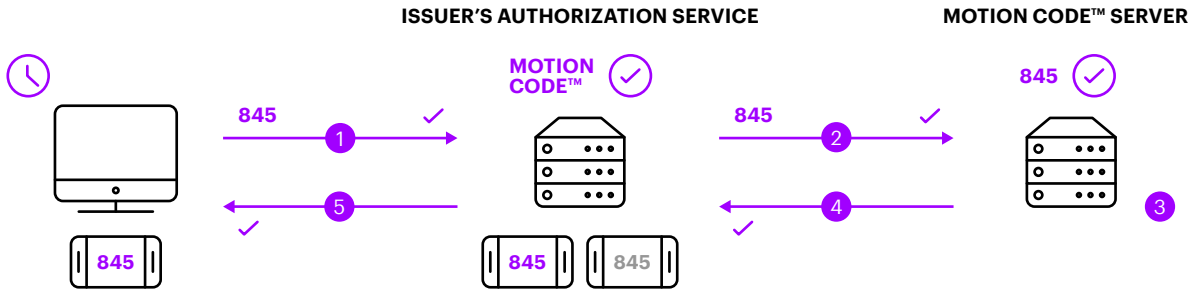
Developed by French security company IDEMIA, it specifically targets CNP fraud by focusing on one aspect of buying by card: the static three-digit CVV/C security code on the back of every debit and credit card, and which the buyer must provide to authenticate the payment.

IDEMIA's approach uses a dynamic CVV/C number replacing the static one, which changes the card's CVV/C number every three or four hours. That's useful not least because a criminal who steals the card data has less than few hours in which to use that information or sell it.

The bank can also analyse this dynamic CVV/C number and that from other compromised cards to identify patterns and pin-point places and establishments where fraud is originating, putting pressure on businesses to identify and report employees who are involved in stealing card data. In that way, Motion Code combines both a protective element and a deterrent one, with criminals having an extremely short window of opportunity in which to capitalise on their crime.

For consumers, there is no change to the way they buy online, because they are used to providing a CVV/C code for purchases. Merchants benefit because of the reduced fraud and they can retain their existing checkout processes. And banks win by cutting financial, time and reputational losses related to fraud.

MOTION CODE™ is a solution combining a card and a server software



1. Card data (PAN, expiry date and MOTION CODE™) sent "normally" via Payment Service Provider up to the issuer's authorization server, just as a transaction with a normal" card
2. Card is recognized as a MOTION CODE™ one by its PAN or BIN: as a result, CSC check is routed for validation towards the IDEMIA MOTION CODE™ server
3. The IDEMIA, server compares the MOTION CODE™ submitted with the one it calculates
4. Result (Valid/Invalid) is routed back to the issuer server
5. Transaction is approved/rejected

How Motion Code works. Source: IDEMIA presentation.

A NEW ERA OF ANTI-FRAUD SOLUTIONS

Motion Code, then, constitutes one innovative solution in efforts to combat fraud—others that banks should use to further enhance and bolster security include transaction controls, artificial intelligence and data analytics. Additionally, developments by banks with strong digital offerings can augment such solutions by offering the cardholder in-app features such as the ability to turn payments on and off, and to set limits.

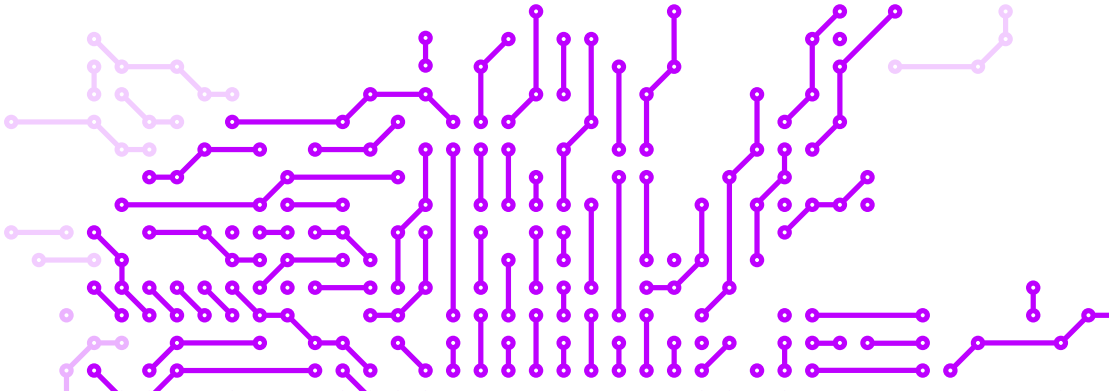
3DS has recently had a makeover, and banks are expected to start supporting 3DS 2.0 this year.[19] The improved version sends more information to the cardholder's bank, allowing the bank to analyse that data and decide whether the purchase is low-risk, in which case the transaction is processed, or whether it constitutes a higher risk—at which point the customer must provide more information. In low-risk cases, then, 3DS 2.0 will provide a frictionless cardholder experience, though that will not be true for all purchases.

Apple takes a bite at cutting card fraud

Apple recently announced it would launch a numberless credit card in the U.S. in 2019, in conjunction with Goldman Sachs and Mastercard.[18]

Security is one of the card's marketing points: the card number is stored in the cardholder's iPhone, with which it works (via Apple Pay) to generate a one-time code for each purchase, using the cardholder's fingerprint or facial recognition. The cardholder is also sent a physical card—which has no numbers on the front or back—for use where Apple Pay is not accepted.

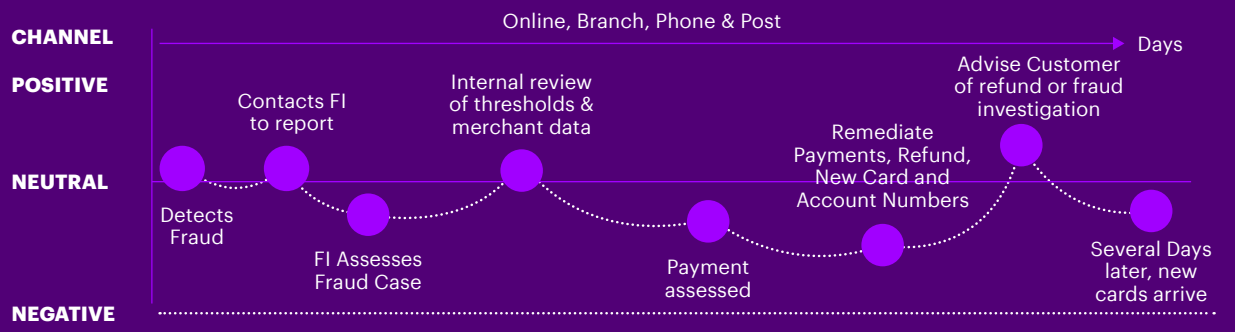
A key criticism of Apple's approach is that online shopping requires the traditional combination of a credit card number, a name, an expiry date and the three-digit CVV code, so it's not yet clear how the Apple Card will work for the majority of online purchases. In addition, it requires the user to open the app to receive their token. And it is a solution that might not work for all markets.



CUSTOMER EXPERIENCE OF FRAUD REMEDIATION

Where are the hidden costs? How much does a fraud case cost Operationally—in addition to $$ of fraud transaction.

The financial costs are not insignificant: chargeback fees can range from US$5-30 per transaction in the U.S.,[20] with merchants also liable for further fees should a case go to arbitration. Other costs include the time spent by all parties in resolving issues, and fees from other parties including payment gateways.



CUSTOMER EXPERIENCE	Informed about fraud or detects unusual transaction	Confused by jargon, limited guidance through process	Small amount of information provided, Manual input required	Limited information provided to customer	Accounts cancelled, new information provided to customer	Sometimes confusing information provided but fraud transaction refunded	Small manual input required, Had to find card to verify correct account number
IMPACT	No strong brand connection/loyalty to FI						

4. THE TIME TO ACT IS NOW

In cases of card fraud, the cardholder is typically the first party to realise fraud has taken place.

They then get in touch with the bank and raise a dispute—which is hardly a smooth process. The more banks can do to mitigate fraud in the first place, the better, not least because the crime can see customers lose faith if they feel helpless in the face of it or believe their bank offered insufficient or no protection.

At the same time, banks in Australia—coming off the back of the Royal Commission's findings—have an opportunity to rebuild their reputations in the public eye by providing innovative, secure ways for customers to stay safe in the evolving world of digital payments. Even if such actions don't benefit the banks' bottom lines, tackling the rise in the amount of card fraud that consumers and merchants are exposed to would be sensible.

Financial institutions, therefore, have a commercial and relationship incentive to act —not least as card fraud continues to climb, albeit at a reduced rate. Additionally, those organizations that invest in digital security will become market differentiators, creating value for themselves and their customers.[21]

The fact is that, although all parties in the digital payments sphere have a responsibility to combat card fraud, the lion's share of that rests with banks—and with more than half-a-billion dollars of card fraud a year in Australia alone there is clearly room for improvement. Banks should look at the options available in order to see how they can play a more effective role.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is **www.accenture.com**

About the Author

Graham Rothwell
Managing Director,
Accenture Financial Services
Australia and New Zealand
g.rothwell@accenture.com

References

1 CNP Fraud mitigation framework – Defining an approach to reduce the growing level of online card fraud in Australia.

2 This figure excludes fraud on proprietary debit cards, which totalled about A$14m (about 2.4 percent of all card fraud) in this period, according to the Australian Payments Network. The organization does not break out transaction value for proprietary debit cards versus other cards; therefore, the total figure of A$767 billion also includes legitimate transactions on proprietary debit cards.

3 Steps to take when shopping online over the Christmas period, Australian Payments Network media release (December 18, 2018).

4 Ibid.

5 Ibid.

6 The Scope of the Card Not Present (CNP) Fraud Problem, Accenture (June 27, 2018).

7 Retailers to Lose $130bn Globally in Card-Not-Present Fraud Over the Next Five Years, Juniper Research (January 2, 2019).

8 FICO Survey: 3 in 4 APAC Banks Believe Fraud Will Increase in 2019, PR Newswire (April 16, 2019).

9 Australian Payment Card Fraud 2018, Australian Payments Network (2018).

10 Chip-and-pin 'cuts fraud by 13%,' BBC News (March 6, 2006).

11 Steps to take when shopping online over the Christmas period, Australian Payments Network media release (December 18, 2018), op cit.

12 Trends in Payments, Clearing and Settlement Systems, Reserve Bank of Australia (2018).

13 How Australians Pay: New Survey Evidence, Reserve Bank of Australia bulletin (March 2017).

14 Stripe Snapshot: Online Fraud Trends and Behavior, Stripe (December 2017).

15 Fraud Statistics Jul 17 – Jun 18, Australian Payments Network.

16 Steps to take when shopping online over the Christmas period, Australian Payments Network media release (December 18, 2018), op cit.

17 The Perfect Secure Payments Storm, Pymnts.com (November 1, 2017).

18 Introducing Apple Card, a new kind of credit card created by Apple, Apple press release (March 25, 2019).

19 3D Secure 2, A new authentication standard, Stripe (April 15, 2019).

20 Unmask Digital Fraud Today: Boosting Customers' and Companies' Defense Against Digital Fraud, Accenture (2018).

21 Ibid.

Disclaimer: This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2019 Accenture.
All rights reserved.

Accenture and its logo are trademarks of Accenture.

191125