accenture

UNMASK DIGITAL FRAUD. TODAY.

BOOSTING CUSTOMERS' AND COMPANIES' DEFENSE AGAINST DIGITAL FRAUD

FS
PERSPECTIVES

CONTENTS

Digital convergence has transformed the marketplace. The new-age consumer is spending more time on "virtual platforms" and prefers "digital conversations" (cashless and seamless payments).

But are these "digital conversations" secure? The future decidedly lies with businesses that can answer confidently in the positive.

FRAUD IS ALIVE. FRAUD IS SMART. AND FRAUD IS HERE TO STAY. ARE YOU?

When EMV (Europay®, Mastercard® and Visa®) chips were first introduced, the world heaved a sigh of relief—it looked like we had finally won the battle against card-related fraud!

Little did we know that the war was far from over.

Undeterred by the advances in technology, the new-age hacker unleashed a new kind of online fraud—card-not-present or CNP—which took the world by storm. It made both financial institutions and customers extremely prone to online data fraud. The fallout was larger than expected.

Banks were flooded with dispute claims and weighed down by chargebacks. And years later, financial institutions are still reporting billions of dollars in losses.

FRAUD IS STRATEGIC. FRAUD IS INNOVATIVE. AND MOST OF ALL, IT IS DETERMINED. ARE YOU?

THE e-FUTURE IS HERE

Digital convergence, the smartphone revolution and affordable, high-speed Internet have together transformed the payments market. They have given financial institutions unprecedented access to consumers—quite literally, enabling them to reach into their pockets. And consumers, on their part, have been quick to adapt to the new marketplace.

While companies have been successfully riding the e-wave, there's been a simultaneous rise in the tide of "digital fraud", specifically, card payments fraud. Consider the following:

2018

Global card losses associated with transaction frauds are expected to cross US$31.3 billion.[1]

2017

Card fraud cases increased by 3.1 percent in Australia, with losses amounting to A$538.2 million. Of these, 82 percent were CNP fraud cases.[2]

2016

Card-not-present (CNP) fraud increased by 40 percent[3] in the US, with consumers bearing up to US$16 billion in losses. In Japan, it rose by 17 percent to JPY140.9 billion[4] (US$1.23 billion), and Australia recorded A$418.1 million[2] in CNP losses, about 78 percent of the total card fraud losses.

If financial institutions do not find a way to prevent fraud, there is a real risk of losing credibility and thus consumer trust and associated business. Such risks will also discourage companies from fully leveraging the amplified reach of digital platforms. Alternatively, investments in digital security will become a market differentiator, creating business value for companies that take a proactive stance.

This whitepaper outlines some key trends in the digital payments market and best practices financial institutions can adopt to tackle fraud and secure digital transactions.

DIGITAL FRAUD GOES SMART

Even as financial institutions and businesses adopt the latest strategies to make digital payments more secure, the nature of digital fraud continues to evolve.

The new-age hacker is using more sophisticated, innovative ways to obtain valuable customer information and login credentials to hack into accounts.

CRIMEWARE

In July 2017, approximately 143 million[8] US citizens, roughly half of US citizens, lost their security authentication data, including name, address, date of birth and social security number (SSN), in a breach at US-based credit bureau Equifax. The repercussions of this incident will be felt over the years to come.

SMARTPHONE ESPIONAGE

In September 2017, 50 malicious apps were downloaded up to 4.2 million times from the Google Play store,[5] affecting 21.1 million Android users. Google immediately removed these apps. But a separate attack by the same group affected 5,000 devices.[6]

POINT-OF-SALE MALWARE ATTACK

In September 2017, approximately 5 million customer credit card numbers were stolen from US-based fast food chain Sonic.[7] The hackers used a malware that duplicates information when a card is swiped at the point of sale (POS) and transmits it automatically to them.

It is evident that the new-age hacker is moving away from those susceptible to direct bank interventions and increasingly targeting consumers by stealing their identity or taking over their accounts through POS malware attacks.

DIGITAL FRAUD HAS DIFFERENT FACETS

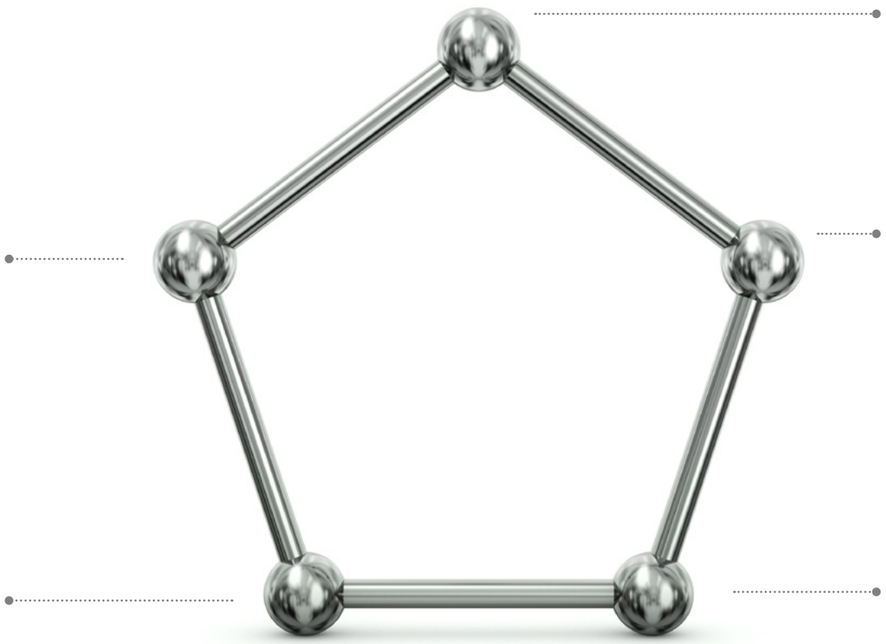
Over the years, hackers have developed multipronged strategies to identify and exploit systemic weaknesses and vulnerabilities. Common types of fraud in digital transactions include the following:

MALWARE

It refers to a computer program that, when installed on a device, can collect data or information for financial transactions. This malware can automatically perform transactions on behalf of customers after hacking into a legitimate session or stealing credentials, including second-factor authentication.

PHISHING

It refers to a method for gathering personal identifiable information (PII), using deceptive e-mails and fake websites that can be used to access customer accounts.



CARD NOT PRESENT (CNP)

CNP or remote purchase fraud involves the fraudulent use of card details obtained through:

- Skimming
- Digital attacks
- Unsolicited e-mails or calls

Card details are used to make purchases over the Internet or by phone or e-mail.

COUNTERFEIT CARD

It refers to a fake card created using compromised details from the magnetic strip of a genuine card.

ACCOUNT TAKE OVER (ATO)

A hacker poses as a genuine customer, takes control of an account and makes unauthorised transactions.

DIGITAL FRAUD IS SHIFTING GEARS

A burgeoning e-commerce sector has provided further impetus for fraud. A Javelin Strategy report forecasts that by 2020, the market value of e-commerce in the US will rise to nearly US$650 billion—or 12.4 percent of the country's total retail volume.[9]

To deal with the sheer volume and variety of data, financial institutions have been adopting various measures to make the digital payments landscape more secure. This has provided an impetus to the new-age hacker to shift gears and find new and innovative ways to target consumers at the POS.

The hacker is also a step ahead—strategising faster than financial institutions can react and quickly switching to alternative methods—something banks are yet unable to do. Here's a case in point.

CASE IN POINT

The introduction of the EMV (Europay®, Mastercard® and Visa®) chip in the past few years was a welcome respite as it helped banks prevent fraud at the POS to an extent. The microprocessor chip, which is embedded in cards and can store and protect user data, quickly became the new global standard for credit and debit card payments. Following its rollout, for a while, it looked like the scales had tipped.

But soon, financial institutions began noting an increase in CNP fraud (those that can be carried out by phone or e-mail, or over the Internet and do not require a physical card for payments). The US alone saw an 81 percent increase in CNP fraud[10] over POS fraud, in 2017.

POS FRAUD ↓ ↑ **CNP FRAUD**

The rise in CNP fraud cases turned out to be a larger problem—the banks started getting flooded with dispute claims. These needed to be further evaluated for the possibility of chargebacks that were intended to protect the cardholders from unauthorised charges due to fraudulent transactions in the first place.

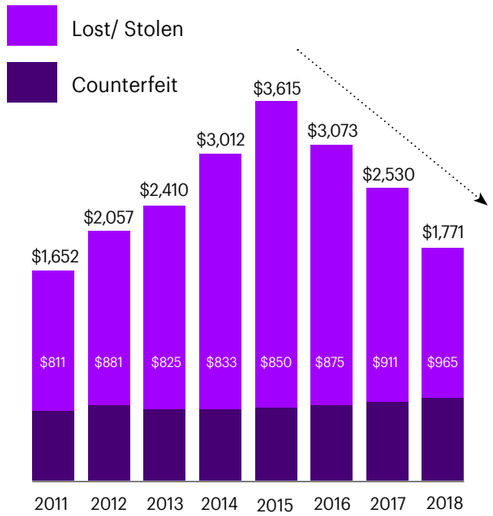
Banks incurred processing charges ranging between US$5 and US$30[11] per chargeback. This has added to the losses for merchants—even higher than the initial dispute amount—as the charges include payment gateways, the processing fee by the acquiring bank, network and interchange fee.

MORE LOSSES

- By 2020, global e-commerce chargeback losses are expected to rise to US$31 billion.[11]
- By 2018, gains due to decrease in card-present fraud are expected to be completely overshadowed by the increase in losses due to CNP fraud (see figure below). With the implementation of EMV chip technology, CNP fraud losses are forecast to double from US$3.1 billion in 2015 to US$6.4 billion in 2018.[12]

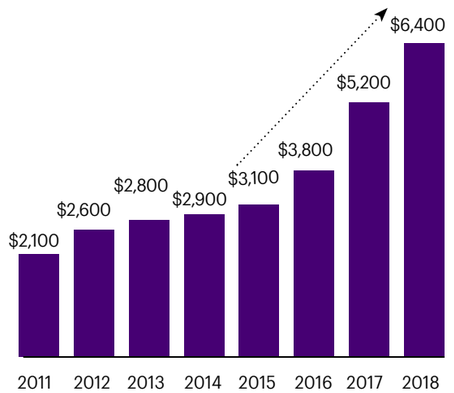
US CARD PRESENT FRAUD LOSSES [2011-2018]

The expected reduction in CP is due to the implementation of EMV in October 2015....



US CNP CREDIT CARD FRAUD LOSSES (2011-2018)

..but the EMV implementation in the US is expected to lead to an increase in CNP fraud



Source: FT Partners Research, quoting Aite group interviews with payments networks and 18 large US issuers, April to May 2014 (figures in US$ millions)

DID YOU KNOW

HIGHER THE TRANSACTION VALUE, GREATER THE CHANCES OF FRAUD

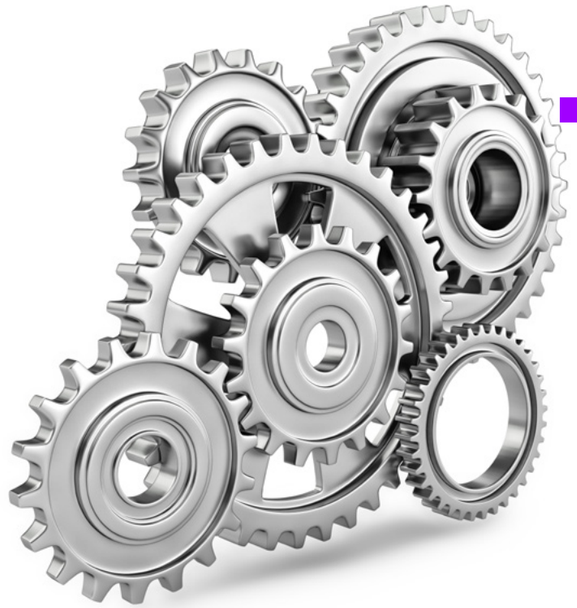
In 2017, transactions valued at more than US$500 had a fraud rate 22 times higher than those valued at less than US$100, globally (11.64 percent and 0.52 percent, respectively).[13]

It takes an average of 53 days to detect fraudulent activity in ATO cases, while it takes an average of 30 days to detect other fraud types.[9]

ATO fraud losses are higher in those merchants earning US$1 million or more annually—up to the mark of US$285,000 annually.[9]

Data breaches that led to ATO accounted for losses up to US$3.3 billion globally in 2017.[13]

Consumers spend US$290 out-of-pocket expenses and 15 hours on an average to resolve fraud.[10]



DIGITAL FRAUD IS ACCELERATING

CURRENT TRENDS

According to the Nilson report,[14] global card fraud losses grew to approximately US$22.8 billion in 2016. In the next four years, Juniper Research[15] predicts losses up to US$71 billion due to CNP fraud, with North America, the Far East and China accounting for 80 percent of these fraud cases.

1

TREND 1:
DIGITAL TRANSACTIONS ARE ON THE RISE

As per an e-Commerce Foundation report, global e-commerce turnover grew by 17.5 percent to reach US$2.7 trillion in 2016. In the Asia Pacific region, it is estimated to have grown by more than 28 percent to US$1.3 trillion. In South-east Asia, online transactions are predicted to rise by 100 percent to US$158.9 billion in 2021 from US$83.4 billion in 2016.[16]

According to the US Federal Reserve Payments Study 2017,[17] total card payments increased at an annual rate of 7.4 percent by number and 5.8 percent by value, from 2015 to 2016. Total card payments in the US grew from US$103.5 billion with a value of US$5.65 trillion in 2015 to US$111.1 billion with a value of US$5.98 trillion in 2016.

2

TREND 2: WITHIN DIGITAL TRANSACTIONS, CNP TRANSACTIONS AND FRAUD ARE INCREASING

CNP transactions are increasing globally, and CNP fraud is growing at an even faster rate. CNP transactions account for 60–70 percent of all card fraud in many developed countries, according to Juniper Research.[18] In the UK, spending on e-commerce has reached £248 billion, with CNP fraud losses at £309 million in 2016.[19]

In the US, fraud losses associated with CNP transactions already account for more than 50 percent of total losses due to fraud.[20] The US Federal Reserve Payments Study 2017[17] also expects CNP transactions to continue to increase for credit, debit and general-purpose card payments by:

TYPE	INCREASE IN VOLUME	INCREASE IN VALUE
Credit card payments	1.5 percent	16.6 percent
Debit card payments	1.4 percent	14.9 percent
General purpose card payments	3.1 percent	15.6 percent

3

TREND 3: WITHIN CNP FRAUD, FRAUDULENT USE OF ACCOUNT NUMBERS IS INCREASING

The discovery of a single file on the Dark Web that contained 1.4 billion unencrypted login credentials in 2017 highlighted the potential scale of ATO fraud.[21] Among the types of CNP fraud, ATO fraud is particularly dangerous because the bank cannot distinguish the legitimate account holder from the hacker. Large-scale data breaches like the one at Equifax provide hackers a goldmine of credentials to test across the web.

The percentage share value of remote card fraud increased from 46.2 percent in 2015 to 58.5 percent in 2016,[17] triggered by an increase in the share of remote payments in total general-purpose card payments. As EMV chip cards led to a reduction in card skimming, hackers also shifted their focus to ATO fraud. According to data from Javelin Strategy & Research,[22] at least 15.4 million consumers in the US were victims of identity theft in 2016—up 16 percent over that in the previous year. In 2016, ATO fraud victims spent 20.7 million hours resolving their cases.

Further, among the types of CNP fraud in the US, the highest increase was seen in fraudulent use of account numbers—from 39.2 percent in 2015 to 44.2 percent in 2016—according to the US Federal Reserve Payments Study 2017.[17]

According to Australian Payments Network (AusPayNet), CNP fraud accounted for more than 80 percent of all card fraud in Australia between July 2016 and June 2017, resulting in up to A$443 million in losses.[23] In emerging economies such as South Africa, the South African Banking Risk Information Centre[24] reports that credit card fraud increased by 1 percent (from R434 million in 2016 to R436.7 million in 2017), with CNP fraud continuing to lead the gross fraud losses, up 7.4 percent from the previous year, and accounting for 72.9 percent of the losses on issued credit cards.

FUTURE TRENDS

Digital wallets have disrupted the market by providing a seamless experience across various devices and online platforms—integrated as gateway services (Visa Checkout©) on communication channels such as Facebook Messenger©—to support commercial activities. New payment providers (such as Apple Pay) act as intermediaries between the web browser and banking sites to facilitate online shopping. Banks are, therefore, unable to detect the middleman, leading to fraud and subsequent losses—likely to be borne by the payment provider.

According to WorldPay,[25] by 2020, mobile wallets will surpass both credit and debit cards in the US, and in-store mobile payments will exceed US$500 billion. As per Juniper Research,[15] fraudulent CNP physical goods sales will reach US$14.8 billion annually by 2022.

TREND 1: BEWARE OF BOT ATTACKS

The use of artificial intelligence (AI) bots is likely to drive fraud in mobile payments. Bots can impersonate legitimate users, mimic human behaviours and convincingly circumvent fraud controls. In 2017, fraud by bots in digital advertising touched US$6.5 billion, globally.[26]

TREND 2: FRAUD HAS GONE SOCIAL

Over the past few years, social media sites have grown to become hotbeds for the new-age hacker. Such sites serve as data-harvesting zones for scammers and an ideal platform for peddling bogus shopping deals and coupon scams.

With e-Shopping and banking growing on social media sites such as Facebook, providers will need to perform fraud detection and respond accordingly.

TREND 3: SPOT THE FAKE (GENEALOGY WEBSITES)

Another trend is that of fraud through fake “genealogy” websites. Scammers target people who are interested in ancestral research and tempt them to register on their website. Unwary customers take the bait and share their credit card information and SSN.

TREND 4: GOING CONTACTLESS

Financial institutions are turning to emerging technologies to prevent fraud. For instance, they have rolled out contactless cards, which are based on secure elements payment technologies such as near field communication (NFC) and host card emulation (HCE). Next, we are likely to see the use of Bluetooth Low Energy (BLE) technology with NFC and HCE to prevent fraud.

In the future, adoption of these new technologies is expected to rise as more users realise their advantages: convenience and quicker payment checkout.

In the US, the share of retailers using contactless payment service rose from 4 percent in 2014 to 35 percent in 2016—that is 4 million contactless POS payments.[27] As per Juniper Research,[28] the combined market share of NFC-enabled Apple Pay, Samsung Pay and Android Pay will reach 56 percent of total mobile contactless payments by 2021.

Similarly, by 2020, 62 percent of wearables will have a payments functionality, driven by an increase in demand for contactless payments.[29] An IDC report[30] predicts voice-based payments through connected voice-enabled devices (Amazon Alexa©, Google Assistant©) will initiate US$150 billion transactions in 2018.

With more and more consumers linking their bank accounts to voice-enabled devices, wearables or cars, there is a growing need to secure internet of things (IOT)-based payment commerce to prevent fraud.

DIGITAL FRAUD IS EVOLVING, BUT THERE'S A WAY TO BEAT IT

Digital fraud is an evolving entity—and is here to stay. Financial institutions must stay alert to stay ahead of the game, and treat fraud detection and prevention as ongoing initiatives. They must proactively deploy intelligent systems that can detect fraud, while ensuring these systems do not dampen the customer experience or hamper the digital payment process.

So, what can companies do? Adopting available measures and exploring emerging technologies can prevent fraud to a large extent. Here's a quick guide:

AVAILABLE MEASURES

3-Domain Secure (3DS) Layers are real-time authentication services in transaction communication that allow issuer banks and merchants to interchange the data provided by customers for authentication. Verified-by-Visa© or Mastercard Secure Code© are examples of 3DS protocols where transactions are initiated and authorised after checkout through a password or dynamic one-time password (OTP) received as a text message on the user's mobile and e-mail account.

The challenge with 3DS protocols, however, is that the information needed for enrolment (for example, SSN) is readily available in the grey market and can be illegitimately used by hackers. If the card is already enrolled online, a simple key logger can give the hacker access to the user's password.

Address Verification Service (AVS) is a mechanism that can effectively limit fraud and chargebacks. AVS verifies the information provided by a cardholder with that available with the issuing bank, along with other factors (such as card number and expiry date).

Once the information is verified, the issuing bank sends an AVS code to the merchant's payment gateway. The challenge, however, is that sometimes even genuine authorised transactions get declined because of personal AVS preferences. From the merchant's perspective, acceptance of failed AVS transactions could lead to higher processing fees.

Tokenisation has been adopted as a secure measure to prevent digital fraud. It prevents the user from giving away payment credentials for each online transaction. If the credentials are compromised, random amounts of funds can be debited from the user's account. As the credit card number is not stored at the POS but parsed directly from the user at the payment gateway, the digital payment is secure and the potential for data breach and fraud decreases.

From the merchant's perspective, full tokenisation secures the card information with the tokenisation provider, including PII, using data security platforms with payment channels (such as a cash register, NFC, mobile payments), using a 'decision engine' that alternates the card number for a single use or creates limited set of tokenised card numbers to secure the information.

Two-factor Authentication (2FA) is widely used for securing online transactions. The user logs into a portal with the help of a password and receives a dynamic OTP via text message on a registered mobile number to authenticate the transaction. This makes it trickier for a hacker, who requires both the cardholder's login password and phone to access the account. When 2FA is used intelligently and sparingly, it can effectively circumvent ATO fraud. However, in case it is used aggressively, it might interfere with the user experience.

EXPLORING THE NEW

"Behavioural analytics" and "AI" are becoming increasingly popular in the context of fraud detection and prevention as they have the potential to benefit both banks and merchants.

Behavioural analytics helps both merchants and issuers implement fraud mitigation techniques down to the transactional level. It works on a predictive model based on user behaviour along with its peer group in a supervised learning mode with known outcomes. It can detect the exact point at which deviations or anomalies occur in user behaviour at the transactional level and triggers alerts. It can be applied on various payment channels, and using machine learning, it can detect fraud when it occurs.

AI-based machine learning is the decision science of creating and applying complex algorithms over large datasets iteratively to analyse patterns and trends. When combined with real-time adaptive behavioural analytics, it can give financial institutions a competitive edge in detecting fraud. Additionally, AI can automatically learn and update the system based on user feedback.

The future of fraud detection in digital payments lies in **AI-enabled behavioural biometrics**—solutions that can continuously authenticate the user during a session. These solutions analyse several data types combined with user interactions. While static biometrics such as face detection and fingerprint recognition can sometimes fail to authenticate user identity or be stolen and used illegitimately, behavioural biometrics analyse user interactions such as touch, pressure, keyboard pattern and mouse scroll velocity in each transaction. Behavioural biometrics can run as invisible applications without impacting the user experience, apply risk-scoring and offer user selectable step-up authentication. Constant authentication methods are required to provide a seamless user experience, with no forced card enrolments or authentication triggers (such as OTPs). Several unique behavioural variables will be used to identify genuine users in each transaction during the payment session.

According to Mercator Advisory,[31] the technology is set to transform the authentication landscape in the next five to eight years and will eventually become a leading fraud detection mechanism on mobile phones as there are several sensors and data sources available in smartphones.

HOW ACCENTURE CAN HELP

Accenture is a proven partner for delivering smart and intelligent solutions for fraud prevention and management using AI and behavioural analytics. Our solutions reduce false positives and fraud investigation costs and help clients achieve a secure and frictionless customer experience.

HERE'S HOW WE CAN HELP:

• Assess and evaluate your current fraud detection processes in digital payments and create a roadmap for solutions.

• Identify appropriate business use cases, with advice on the selection of AI, machine learning, analytics, biometric technology and product fitment.

• Build a proof-of-concept for select business use cases and execute the fraud prevention mechanism with the help of select tools, and training resources for fraud prevention.

PROCESS MAPS AND OPERATING MODELS

Our detailed process maps and operating models can be used to assess the current state, future state design in tandem with current state, conformance testing and technology deployment for financial institutions.

FRAUD DIAGNOSTIC AND TRAINING

We have led industry best practices in fraud management based on our experience, expertise and regulatory best practice guides. We help firms assess current security measures and provide a blueprint for future design. Our fraud diagnostic tools cover more than 500 attributes in fraud management, and help and train companies to detect and prevent fraud. The training material covers typical fraud scenarios across products and channels.

NEXT-GENERATION FRAUD ANALYTICS WITH AI

Our fraud analytics solution leverages the multiplicity of data sources such as transactional, social, financial, forensic and government records. It combines the automated learning from data with human judgement and feedback, providing significant improvement in business outcomes in fraud investigation. The solution also adapts to changing behaviours and can provide significant improvement in business outcomes, for example, better quality leads for investigation. It also provides innovative identity solutions, and risk-scoring solutions and frameworks with step-up authentication capability.

STRONG INDUSTRY EXPERIENCE

We enable clients to develop a holistic understanding of fraud management and deploy cutting-edge analytic solutions that optimise fraud detection mechanisms by exploiting meaningful internal and external data sources. This significantly lowers operational costs by reducing false positives and increases the efficiency of investigation, while ensuring a smooth customer experience and maximising profits from payment operations.

ALLIANCES

Our extensive capabilities range from accessing and reporting data to advanced mathematical modelling, forecasting and sophisticated statistical analysis. We have more than 20 years of experience in advanced analytics across different industries, and several technological alliances with proven industry partners.

STAYING AHEAD OF THE GAME

The implementation of EMV chips was certainly a strong fraud prevention measure that resulted in a significant drop in the card-present transaction fraud rate. But the ensuing evolution of digital fraud and shift in focus to CNP transactions shows that financial institutions must stay alert and continuously innovate to detect and prevent online fraud.

Fraud will continue to rise and hamper consumers' digital conversations. If financial institutions do not take immediate measures, they risk all that's dear to them—money, time and reputation. Hackers will continue to use the latest technology to attack the various touch-points of the booming e-commerce business.

Be proactive when it comes to fraud detection. Financial institutions must build digital payment platforms with a high degree of accuracy that will not generate false alarms, interfere with the customer experience or be vulnerable to spoofs.

Be innovative and invest in AI and behavioural analytics. An Accenture survey of six leading banks and payment institutions found that they have already implemented measures such as 3-DS, AVS, tokenisation and 2-FA to contain digital fraud, and are now looking at developing AI and behavioural analytics-based real-time, intelligent decision-making platforms to prevent fraud proactively. This will go a long way in helping enterprises secure the future in the digital age.

REFERENCES

1 https://www.accenture.com/t20171012T092409Z__w__/ca-en/_acnmedia/PDF-62/Accenture-Driving-the-Future-of-Payments-10-Mega-Trends.pdf

2 http://www.auspaynet.com.au/resources/fraud-statistics

3 https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

4 https://asia.nikkei.com/Business/Consumers/Japanese-travel-websites-team-up-against-credit-card-fraud

5 https://www.express.co.uk/life-style/science-technology/854529/Android-warning-Google-Play-malware-ExpensiveWall

6 https://arstechnica.com/information-technology/2017/09/malicious-apps-with-1-million-downloads-slip-past-google-defenses-twice/

7 https://www.usatoday.com/story/tech/2017/09/27/sonic-drive-hit-security-breach/708850001/

8 https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

9 https://s3.amazonaws.com/dive_static/paychek/Financial_Impact_of_Fraud_Study_FINAL.pdf

10 https://www.Javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

11 https://chargeback.com/ecommerce-payment-fraud-outlook-2020/

12 https://www.pymnts.com/news/2015/outsmarting-the-cnp-fraudsters/

13 https://www.pymnts.com/global-fraud-index/

14 https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1118.pdf

15 https://www.juniperresearch.com/press/press-releases/retailers-to-lose-$71-bn-in-card-not-present-fraud

16 http://www.experian.com.vn/wp-content/uploads/2017/12/fraud-management-insights-2017.pdf

17 https://www.federalreserve.gov/newsevents/pressreleases/files/2017-payment-systems-study-annual-supplement-20171221.pdf

18 http://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-paymentfraud-wp-2016.pdf

19 http://www.paymentscardsandmobile.com/european-card-fraud/

20 https://emerchantbroker.com/blog/global-card-fraud-grows-20-cnp-fraud-is-on-the-rise-worldwide/

21 https://www.techradar.com/news/huge-database-of-14-billion-credentials-on-dark-web-could-contain-your-login

22 https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

23 http://www.auspaynet.com.au/sites/default/files/2017-12/Payment%20Fraud%20Statistics%20Jun%202017.pdf

24 https://anticorruptiondigest.com/anti-corruption-news/2018/04/20/these-are-the-worst-bank-card-fraud-scamsin-south-africa/

25 http://blog.securedtouch.com/predictions-for-the-mobile-payment-fraud-landscape-in-2018

26 https://www.infosecurity-magazine.com/news/digital-ad-bot-fraud-set-to-reach/

27 https://www.thepaypers.com/expert-opinion/payment-trends-in-the-us-the-emv-migration-and-the-future-of-mobilepayments/771640

28 http://www.kreditwesen.de/system/files/content/inserts/2017/is_oem_pay_the_future_of_contactless_whitepaper_52669.pdf

29 https://www.itproportal.com/features/whats-next-for-wearables-in-2018/

30 https://cardnotpresent.com/voice-commerce-fraud-are-top-2018-trends-in-payments/

31 https://www.mercatoradvisorygroup.com/uploadedFiles/Pages/ForeSight/Authentication%20Foresight-ET-FINAL.pdf

OUR CONTACTS

TALES SIAN LOPES
Managing Director – Finance and Risk Services Lead for Financial Services
Accenture in Australia and New Zealand
tales.s.lopes@accenture.com

DAVID POWELL
Managing Director – Security Lead for Financial Services
Accenture in Australia and New Zealand
d.powell@accenture.com

ANKIT SUNEJA
Associate Manager – Practice Lead for Cards
Banking Industry Practice, Accenture Technology Services
Advanced Technology Centers in India
ankit.suneja@accenture.com

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 specialised 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 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.