

LexisNexis® Risk Solutions 2019 True Cost of FraudSM APAC Study



Philippines Report
September 2019

Research Definitions



The LexisNexis® Risk Solutions 2019 APAC True Cost of FraudSM Study helps Retailers, e-Commerce merchants, and Financial Services businesses grow their revenues safely and manage the cost of fraud, whilst strengthening customer trust and loyalty.

The research provides a snapshot of:

- » Current fraud trends in the Philippine Retail, e-Commerce, and Financial Services markets
- » Key pain points related to adding new payment mechanisms, transacting through web browsers and mobile, and expanding internationally

Fraud Definitions

Fraud is defined as the following:

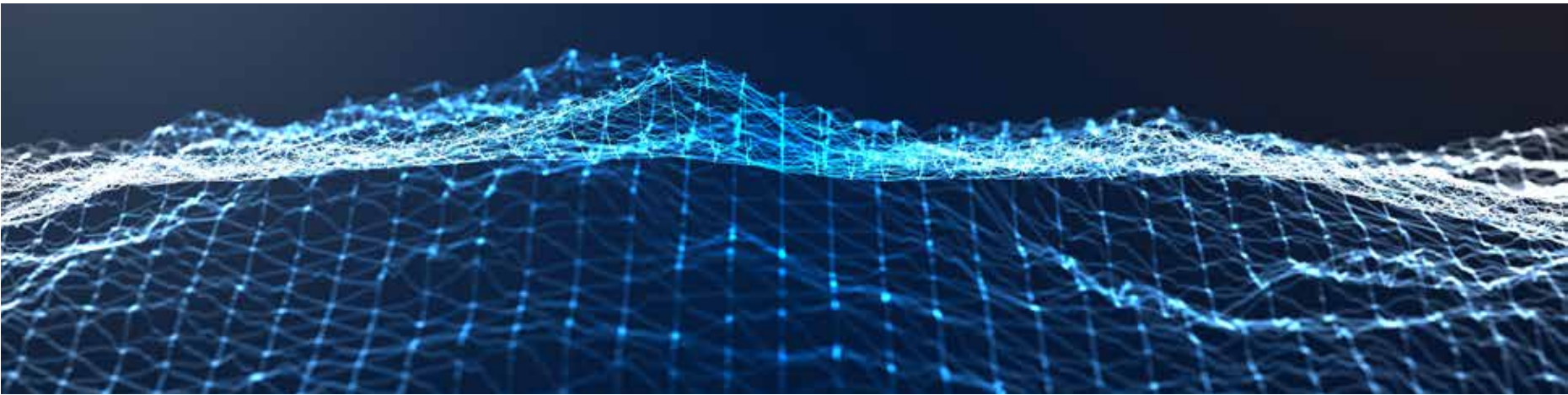
- » Fraudulent and/or unauthorised transactions;
- » Fraudulent requests for refund/return; bounced cheques;
- » Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items;
- » Fraudulent applications (i.e., purposely providing incorrect information about oneself, such as income, employment, etc.);
- » Account takeover by unauthorised persons; and
- » Use of accounts for money laundering.

This research covers consumer-facing fraud methods

- » It does not include insider fraud or employee fraud

The LexisNexis Fraud MultiplierSM

- » Estimates the total amount of loss a merchant/company occurs based on the actual value of a fraudulent transaction



Research Definitions



Key Findings



Recommendations



Summary





Study Data

Study data was collected online and by phone from June to August 2019. 360 surveys were completed with risk and fraud decision-makers, distributed across 4 APAC markets. The following report reflects Philippine results.

	Singapore	Indonesia	Malaysia	Philippines
Retail	30	30	30	30
e-Commerce	30	30	30	30
Financial Services	30	30	30	30
TOTAL	90	90	90	90

Surveyed industries include*:



Retail

May or may not be omni-channel; earn less than 80% of revenues through online channels



e-Commerce

Earn 80% or more of revenues through online channels



Financial Services

Retail/Commercial Banks
Credit Unions
Investments
Trusts
Wealth Management

Across various categories, including:
Apparel/Clothing, Automotive parts, Books/Music, Computers/Software, Digital Goods, Drug/Health & Beauty, Flowers/Gifts/Jewelry, Food & Beverage, General Merchandise, Hardware/Home Improvement, Hotel/Travel, Housewares/Home Furnishings, Office Supplies, Sporting Goods, Toys/Hobbies

*Use of the phrase “surveyed industries” throughout the report refers to Retail, e-Commerce, and Financial Services

Segment Definitions



- Research Definitions
- Key Findings
- Recommendations
- Summary
-

Research Definitions

Key Findings

Recommendations

Summary

Online Channels



Web Browser

Transactions through a computer/web browser



Mobile

Transactions through a smartphone/tablet, using mobile browser, mobile apps, contactless purchase, pay by text, and/or bill to mobile phone



m-Commerce

Transactions specifically through mobile browser and/or mobile apps

Digital



Retailers & e-Commerce Merchants Selling Digital Goods/Services

Includes omni-channel Retailers, but more likely to be e-Commerce Merchants, selling goods or services that are stored, delivered, and used in electronic format:

- » Cloud-based applications
- » Digital services (i.e. Uber, Lyft, AirBnB)
- » Digital subscriptions
- » Downloadable software
- » eBooks, eLearning/online courses
- » eGift cards
- » Electronic tickets (i.e. concerts, sports, events)
- » Media streaming/downloads (i.e. TV, videos, music)
- » Mobile apps
- » Online games/gaming
- » Photos/graphics



Digital Financial Services

Earn 50% or more of revenues through online channels



Research
Definitions



Key Findings



Recommendations



Summary



Key Findings

- 1 The cost of fraud for surveyed industries in the Philippines is 3.46 times the lost transaction value.**
 - » This appears to be driven higher by Financial Services businesses, where the cost of fraud is 4.01 times the value of the lost transaction.
- 2 The mobile channel is contributing to fraud risk among surveyed industries in the Philippines.**
 - » This includes both mobile web browsers and mobile apps.
- 3 Customer identity verification is a key issue for online channels.**
 - » Balancing speed of approval against customer friction is a key difficulty for online channels in general. Limited ability to confirm order location and volume of malicious botnet orders are problematic through mobile. The rise of synthetic identities is an issue for web browsers.
- 4 Businesses in surveyed industries that offer m-Commerce suffer from the cost of fraud. But Digital Financial Services firms (regionally) suffer even more.**
 - » For every fraudulent incident, the cost to businesses that offer m-Commerce is actually 4.04 times the amount of the lost transaction value, totaling fraud costs that are 2.26% of annual revenues. And this cost is even higher, up to 4.09 times the lost transaction amount, for Digital Financial Services firms across study countries.
- 5 Businesses across surveyed industries are not effectively fighting fraud.**
 - » 35% reportedly do not track successful fraud transactions by both channel and payment method. Additionally, an average of 67% of flagged transactions continue to be sent for costly and time-consuming manual reviews.
- 6 The use of more advanced fraud mitigation solutions is limited.**
 - » The use of more advanced solutions, and those geared toward mobile fraud detection, such as Digital Identity, Geolocation, and OTP/2 factor is limited.



1 The cost of fraud for surveyed industries in the Philippines is 3.46 times the lost transaction value.





Research Definitions



Key Findings



Recommendations

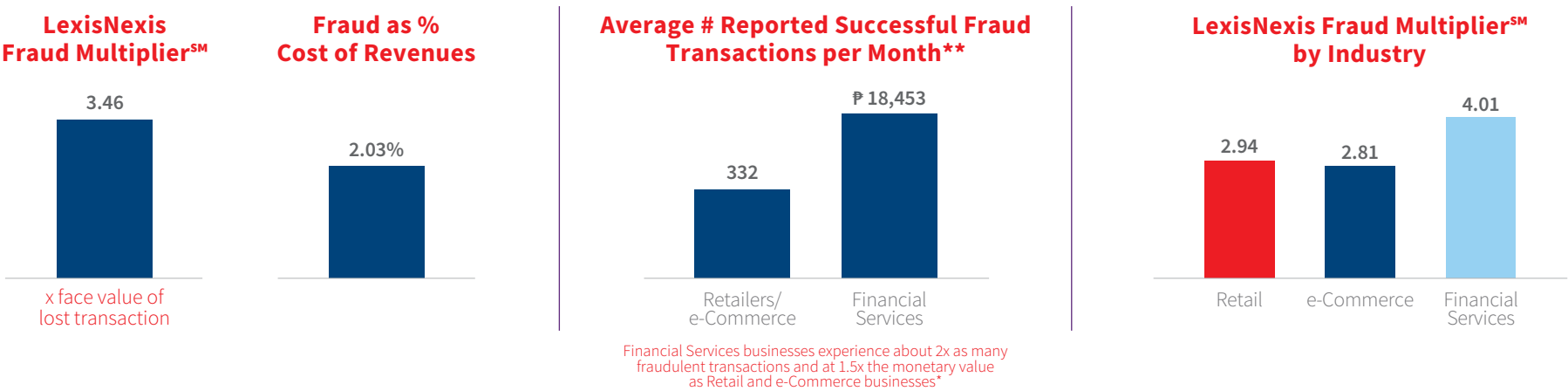


Summary



The LexisNexis Fraud MultiplierSM is 3.46 across surveyed industries.

- » This means that for every fraudulent transaction, the cost to Philippine businesses is actually 3.46 times the amount of the lost transaction value. This translates to fraud costs amounting to 2.03% of annual revenues overall.
- » Country-level fraud volumes and costs appear to be driven up, in part, by the Financial Services sector, where volumes and costs are higher.* And whilst anecdotal (given small base sizes), the cost of fraud for Financial Services is directionally higher in the Philippines (4.01 times the face value of the lost transaction) than in the United States (2.92 times). Some of this could relate to a 78% year-on-year growth in Financial Services attack rates for new account creations in the region.¹
- » The mobile channel, digital goods sales, and limited use of solutions to address specific threats are part of the reason for higher risks and costs.



* CAUTION: small number of cases, data should be used directionally only 1 ThreatMetrix® H2 2018 Cybercrime Report
** Based on self-reported numbers and likely recall; not meant to be exact; may increase or decrease based on seasonality

How is the LexisNexis Fraud MultiplierSM calculated?



- Research Definitions
- Key Findings
- Recommendations
- Summary

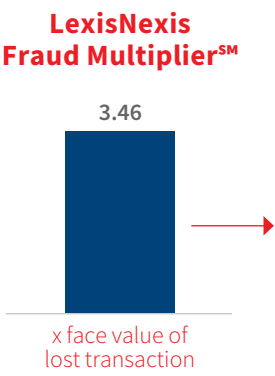


Illustration	Description
Calculating the LexisNexis Fraud Multiplier SM	The total cost for every Rp 1 of fraud, calculated as total losses divided by the amount of fraudulent transactions for which the firm is held liable
Step 1: Obtain average revenue	₱ 20,025,023,724*
Step 2: Obtain fraud as % of annual revenue from Q10	2.03%
Step 3: Calculate total cost of fraud (Steps #1 x #2)**	₱ 406,507,982
Step 4: Obtain % of total losses for lost transaction values (actual values of the fraudulent transactions that occurred) (Q16)	28.91%
Step 5: Calculate actual value of the fraudulent transaction that occurred (Steps #3 x #4)	₱ 117,521,458
Step 6: Calculate total cost for every S\$ 1 of fraud (total cost in Step 3) / (value of fraudulent transactions in Step 5)	\$3.46

**Total cost of fraud includes not only the lost transaction face value for which firms a held liable, but also costs for replacing or redistributing lost/stolen merchandise, fees/interest paid to financial institutions, fees and interest incurred during the application, underwriting, and processing stages, fines and legal fees, labor for investigation, and external costs for expense recovery.



Research
Definitions



Key Findings



Recommendations



Summary



Contributing factors to fraud in the Philippines.



Market Conditions

The risk of fraud is higher through remote channels and the Philippines’ e-Commerce and m-Commerce sections continue to develop:

- » The country has seen countless fraud incidents like ATM card skimming, online scams, and identity fraud.²
- » Though e-commerce still represents around 1% of all sales in the Philippines, the market is expected to grow into double digits in the near future. An improving telecommunications infrastructure and the growing proportion of the population with internet connectivity (especially through mobile phones), are a few factors that are expected to make the country a major player of e-commerce in Southeast Asia.³
- » **Barriers to secure payment methods**; sizeable unbanked population that requires merchants to attract these consumers through alternative payment methods and mobile devices which may not always be secure.

Cybercrime threats:

- » The number of cybercrime cases in the country reportedly increased by nearly 80% last year. Preventing cybercrime remains a challenge, with enforcement agencies having to constantly adjust their strategies because of the rapidly evolving technology used by fraudsters.⁴

2<https://aseanup.com/insights-trends-e-commerce-philippines/>
3<https://www.rappler.com/brandrap/data-stories/225452-reasons-philippines-slow-adopt-e-wallet>
4<https://www.philstar.com/headlines/2019/03/29/1905544/cybercrimes-80-2018>

Transaction Risks

Growth of mobile channel transactions, including high use of mobile browsers and mobile apps that are increasingly targeted by fraudsters. The mobile channel is more risky/less secure.

Risks from mobile browser and mobile app transaction methods.

Those selling digital goods and services are challenged with more real-time need for fraud detection and identity verification given the speed and nature of the transaction (i.e., quickly downloaded, no delivery address to support verification).

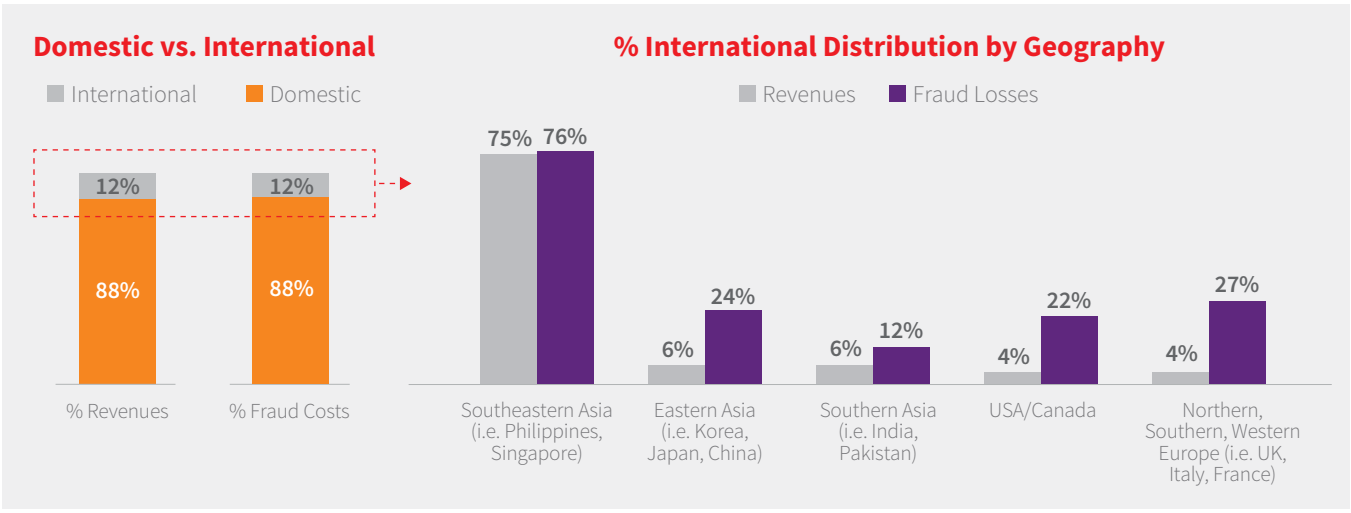
Limited use of risk mitigation solutions that specifically address mobile and digital goods/services risks.





Major revenue and fraud losses come from Philippine-oriented transactions.

- » Where non-Philippine fraud occurs, a majority comes from other Southeastern Asian markets.
- » There is a disproportionate degree of fraud other regions as compared to their revenue contributions. This follows a growing trend with attack dispersion, in which attackers are beginning to target markets outside of their region.⁵



5 ThreatMetrix® H2 2018 Cybercrime Report



2 The mobile channel is contributing to fraud risk among surveyed industries in the Philippines.





Research Definitions



Key Findings



Recommendations



Summary

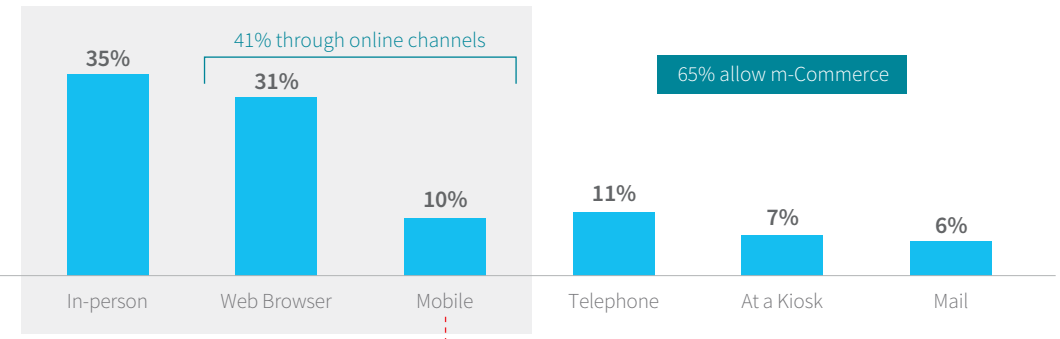


A majority of transactions go through the in-person and online channels.

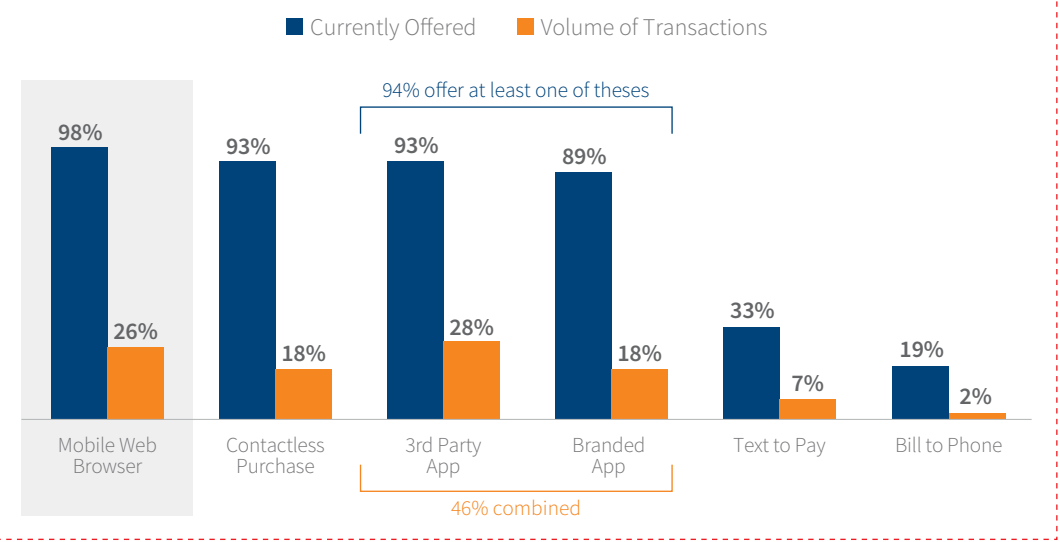
- » Though mobile channel transaction volumes are modest compared to other types, m-Commerce is reportedly growing quickly in the Philippines. 65% of the population is said to be online and using their mobile devices as a “remote control” for commerce and entertainment. As more people go online, internet speeds pick up, and more merchants like Lazada, Alibaba and Shopee enter the market.⁶
- » Among businesses offering m-Commerce, the greatest portion of transactions occur through branded and 3rd party mobile apps, followed by mobile web browsers.
- » Whilst mobile web browsers have historically been considered less secure, fraudsters are increasingly targeting mobile apps at a global level⁷, driven in part by click flooding and botnet attacks, with shopping, gaming and financial apps being hardest hit. These botnets attack devices through malware and can then imitate legitimate transactions coming from a mobile app. Device owners may not even be aware of this.

6 <https://news.abs-cbn.com/business/04/05/18/mobile-remote-points-to-10-billion-e-commerce-market-in-ph-google>
7 <https://www.appsflyer.com/resources/the-state-of-mobile-fraud-q1-2018/>

Average Distribution of Transaction Volume Across all Channels



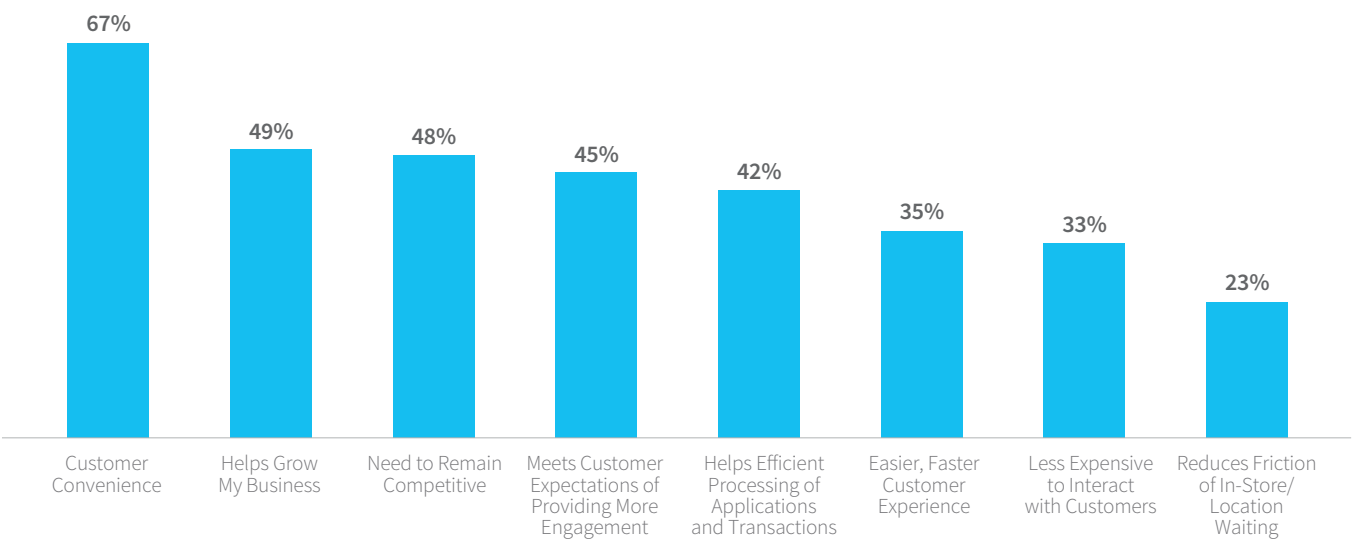
Mobile Methods





Even so, mobile channel risk appears to be an accepted trade-off for providing customer convenience and to grow business.

Reasons For Accepting Mobile Transactions
(among those transacting through the mobile channel)

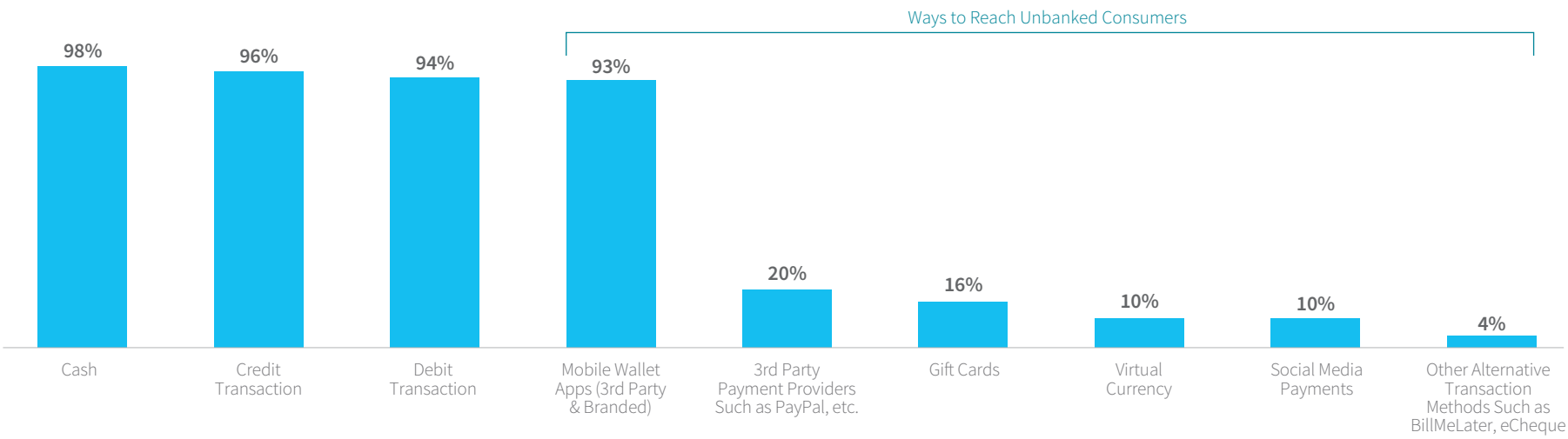




Traditional payment methods remain most often accepted (cash, credit, debit cards), but mobile apps are reportedly accepted just as much, as companies strive to reach unbanked customers.

- » According to a recent survey by the Central Bank of Philippines, 77% of the Philippine population (~52.8 million people) is unbanked.⁸
- » However, the Philippines is said to have a rising middle class and is touted as a mobile-first market, with smartphone adoption at 59%, thanks to affordable phones. Cellular subscription is reported to be 110 per 100 people.⁹ As a result, the Philippine fintech sector is predicted to soon enter “a new phase of development” driven by the large, mobile-savvy, and increasingly well-off generation of Filipinos who will be demanding digital financial services. The list of fintech players looking to cater to the Philippines’ unbanked continues to grow, with hopes to reach an estimated 69% of those who are currently unbanked.¹⁰

% of Organizations that Accept the Following Types of Payment Methods: Among Those with Mobile Channel Transactions*
(*Not necessarily used with mobile channel transactions, since merchants and firms are multi-channel)



8 <https://theaseanpost.com/article/hotbed-fintech-activities>
9 <https://www.rappler.com/brandrap/data-stories/225452-reasons-philippines-slow-adopt-e-wallet>
10 <http://fintechnews.sg/27510/philippines/10-new-philippine-fintech-startups-to-watch-out-for-in-2019/>

3 Customer identity verification is a key issue for online channels.



Research
Definitions



Key Findings



Recommendations



Summary

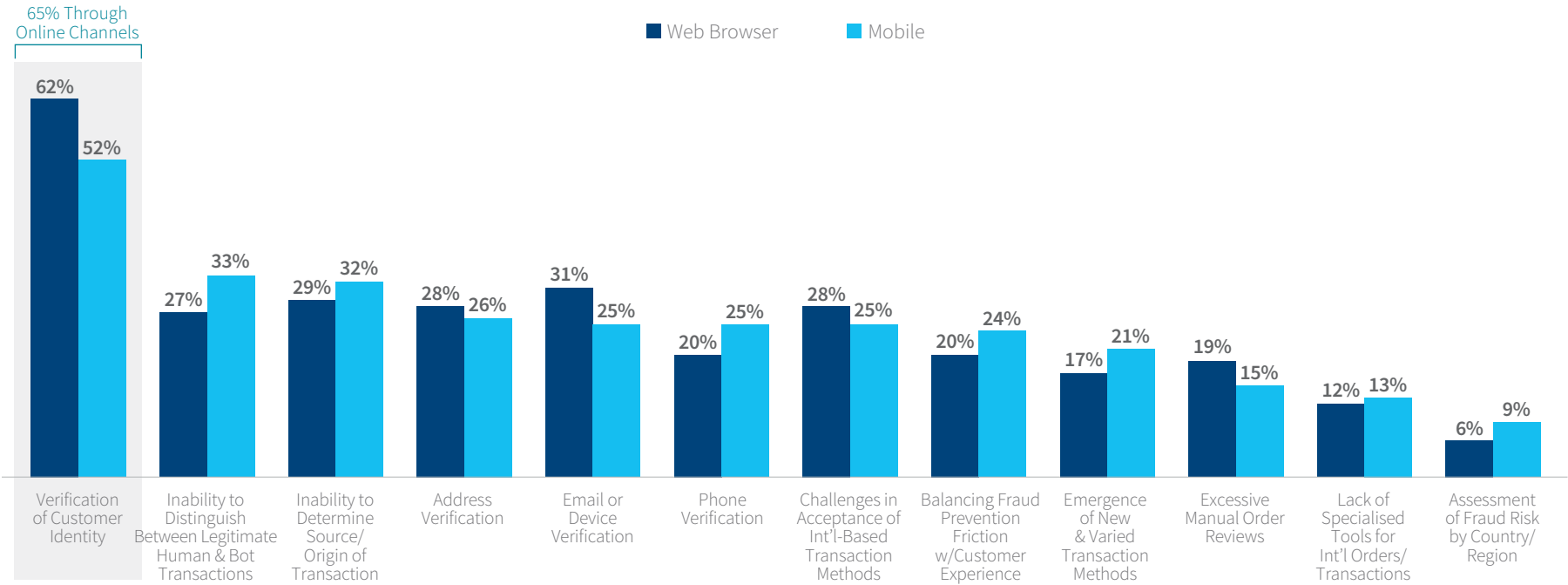




Customer identity verification is a key challenge for online channels.

» Processing e-commerce and m-commerce transactions are further complicated by a myriad of other challenges, which are similar by channel.

Top 3 Challenges Related to Fraud When Serving Customers Through...
(among those transacting through each channel)

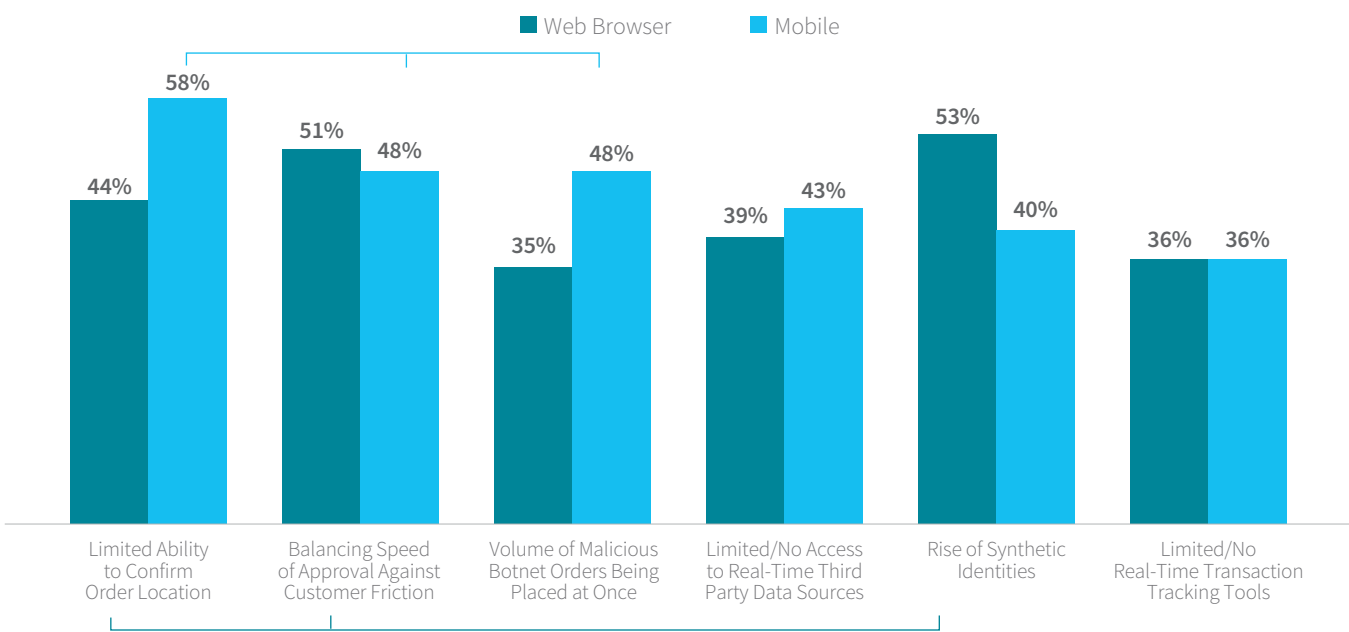




Balancing speed of approval against customer friction is a key difficulty for customer identity verification across both web browsers and mobile.

- » Limited ability to confirm order location and volume of malicious botnet orders are more problematic through mobile. The rise of synthetic identities is more of an issue for web browsers.
- » As prevention technologies have improved to stop activities such as card skimming, criminals are now stealing identities or constructing “fake” people. The availability of personal information online via social media platforms and mobile apps has made it easier for culprits to mix fake and real personal information. 6 in 10 APAC banks reportedly experienced synthetic identity fraud in 2018.¹¹

Top 3 Factors That Make Customer Identity Verification a Challenge Through...
(among those transacting through each channel)



¹¹ <https://sbr.com.sg/financial-services/asia/6-in-10-banks-in-apac-victimised-fake-identities>



Research
Definitions



Key Findings



Recommendations





Summary




Synthetic identities are a serious threat. Their very nature makes it extremely difficult to detect before damage is incurred.

Synthetic identities are comprised of real and/or fake personal information. They are created by using information from either:

 **Multiple real persons** into a single fake identity, with a valid shipping address, tax/insurance/identification number, date of birth, name, etc. – none of which matches any one person. This type may be used for shorter-term fraud gains, such as bigger ticket items.

 **One real person** by using some of his / her information combined with fake data. In this case, the fraudster is likely to be nurturing this identity, using it to establish a good credit history before ultimately “going bad”.

 **No known persons** in which the personally identifiable information doesn’t belong to any consumer. It is entirely fabricated and may be nurtured for longer-term gain and is useful when posing as an underbanked consumer with a less established purchasing footprint (i.e., younger Millennials).



Risks & Challenges

Extremely Hard to Distinguish from Legitimate Customers

Focus on nurturing the identity to mimic a good customer; establishes good credit, pays on-time, etc. before “breaking bad”

Difficult to detect with traditional identity verification / authentication solutions

These are professional fraudsters; they often know the types of information required to gain approval and pass certain checkpoints. Use of real identity data helps them do this.

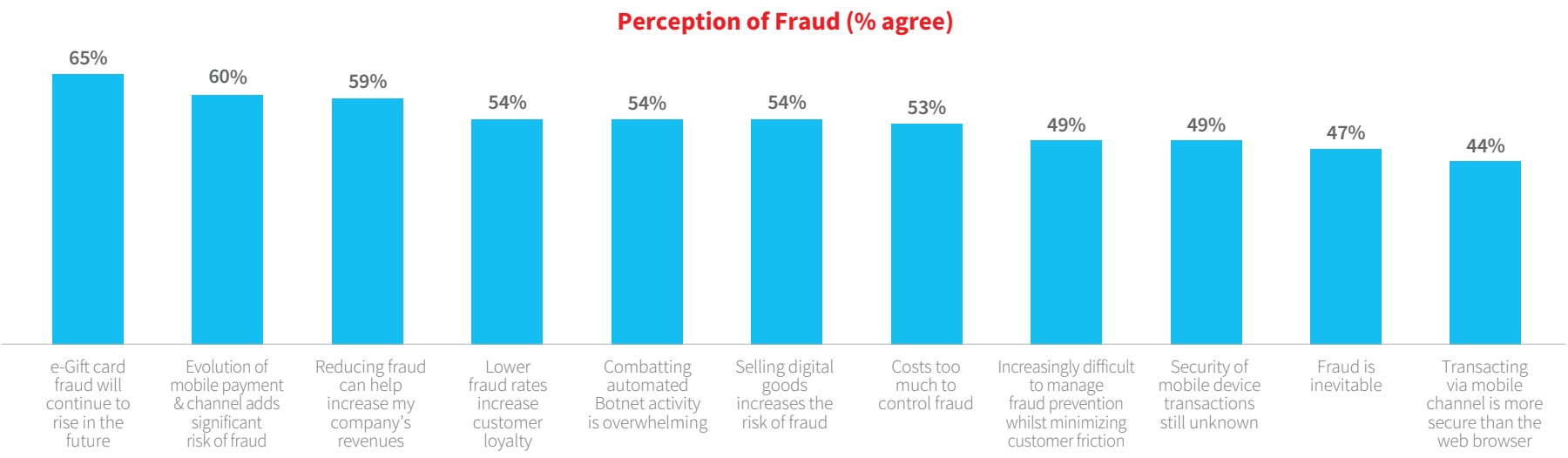
Real customers don’t help; behaviours make it difficult to spot anomalies with current ID solutions.

Consumers have more ways to purchase, from different locations anywhere and anytime. They might share passwords and use different devices at different times. It is harder to make physical and digital connections that distinguish fraudulent from legitimate patterns.



Many across surveyed industries believe that reducing fraud can help to drive revenues and customer loyalty.

- » However, there are also expectations that e-gift card fraud will continue to rise, the mobile channel and selling digital goods add fraud risk, combatting automated botnet activity is overwhelming and fraud is inevitable.
- » This further supports the importance of businesses implementing effective fraud mitigation solutions.



*Asked only of Retail/e-Commerce selling digital goods



4 Businesses in surveyed industries that offer m-Commerce suffer from the cost of fraud. But Digital Financial Services firms (regionally) suffer even more.

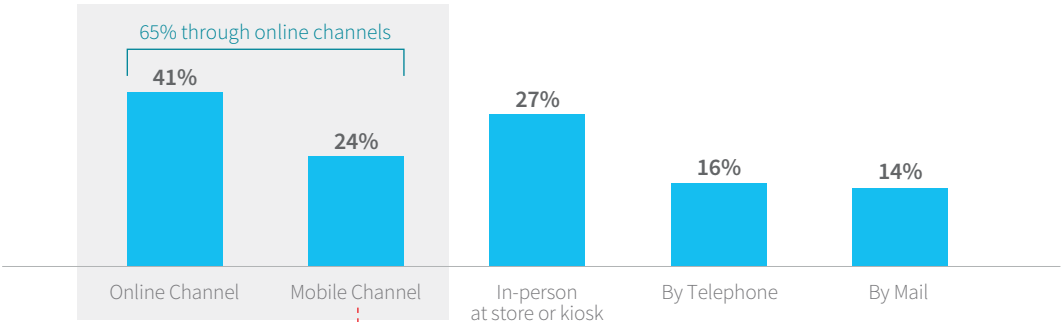




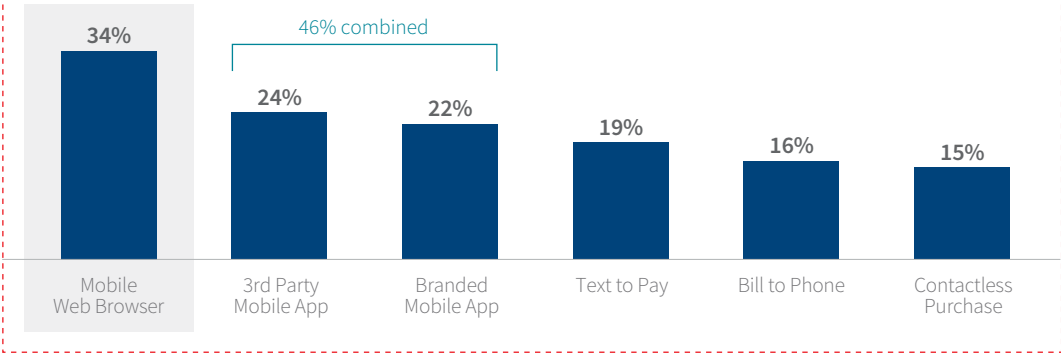
A large share of fraud, approximately 65%, occurs through online channels.

- » Mobile transactions in the region are experiencing a growth in attack rate of 17% year-on-year.¹²
- » Whilst mobile web browsers account for the single largest amount of fraud losses, branded and 3rd party mobile apps account for more, combined. This shows that fraudsters are targeting them, often through click flooding and botnet attacks.

% of Fraud by Transaction Channel
(as % of total annual fraud losses)*



Mobile Fraud by Channel
(as % of mobile fraud losses)*



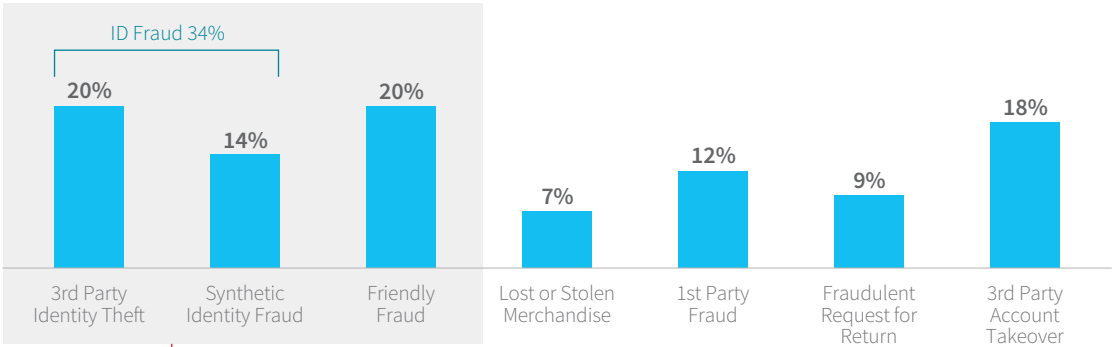
¹² ThreatMetrix® H2 2018 Cybercrime Report
*% can add to more than 100% since answers based on using a channel



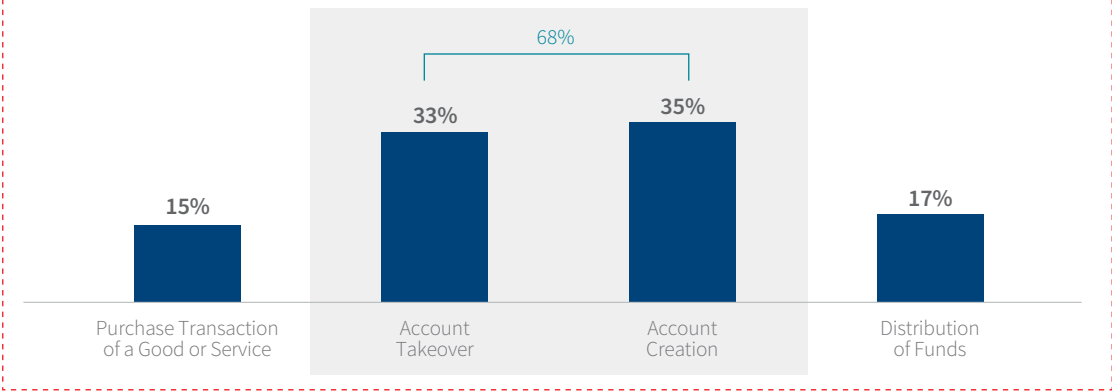
Approximately 34% of fraud losses, on average, can be attributed to identity fraud (3rd party identity theft/synthetic identity).

- » Fraud from account takeovers and fraudulent account creations represents significantly more identity-based fraud than that coming from purchases or transactions.
- » New e-Commerce account creation transactions from Southeast Asia are attacked at a very high rate of 41%. And new account creations attacks in the Financial Services sector have grown by 78% overall, and 105% through mobile devices.¹³

% Distribution of Fraud Losses by Method



Identity-Related Fraud Types



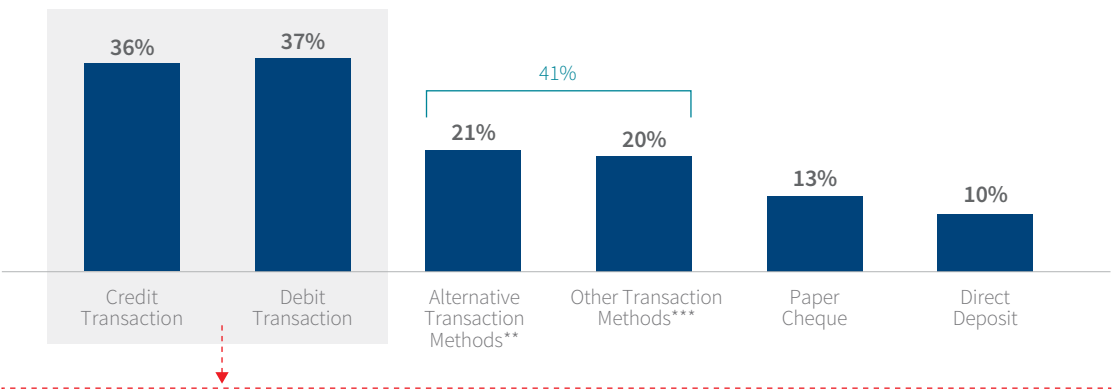
13 Ibid.



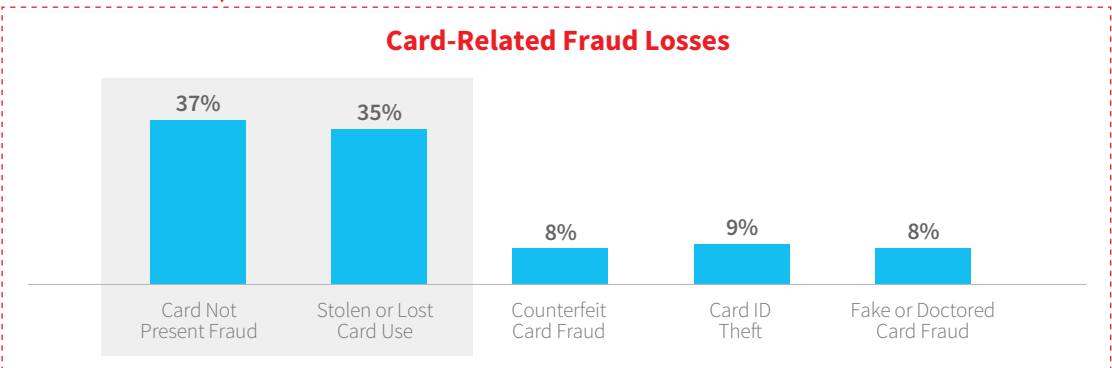
Whilst credit and debit transactions account for most of fraud losses, alternative and other methods (that include web and mobile options) amount to just as much.

- » In 2016, 80,000 fraudulent credit card transactions were recorded, yet not reported to the police. A bank executive disclosed that approximately ₱507 million was lost as a result. Due to rising fraud numbers, members of the banking industry have forged an alliance with the PNP ACG and Information Security Officers Group (ISOG) to form an anti-fraud working group. It has also been suggested that all banks educate their consumers on fraud awareness.¹⁴
- » The Bangko Sentral ng Pilipinas (BSP) is one bank that has issued a guide for credit card owners to avoid being victims of scams, such as card theft, information and identity theft, skimming, phishing, and card replacement scam.¹⁵

Fraud by Transaction Method
(as % of total annual fraud losses)*



Card-Related Fraud Losses

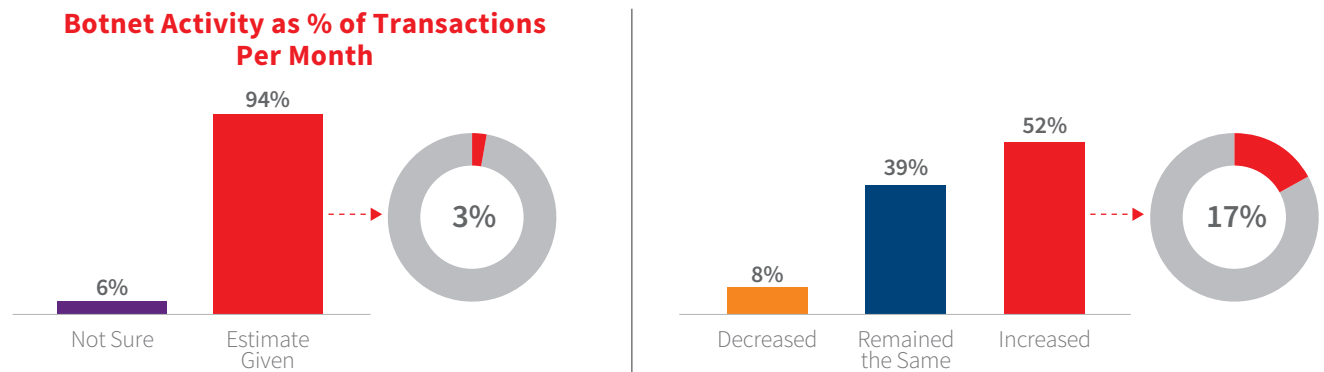


14 <https://business.inquirer.net/226584/credit-card-fraud-cost-consumers-p506m-2016-bank-exec>
15 <https://www.gobear.com/ph/blog/credit-card/credit-card-scams-to-watch-out-for-in-2019>



52% of businesses across surveyed industries have experienced an increase in automated botnet activity over the past year.

» This is a growth of 17% of transactions on average.





Research Definitions



Key Findings



Recommendations



Summary



The combination of these factors contribute to increased risk.



Mobile

- » **Rise of mobile botnet attacks;** malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases¹⁶
- » **Consumer risk behaviours** – using open WiFi networks increases risk of smishing (SMS-based phishing) and man-in-the-middle interception of passcodes used for multi-factor authentication¹⁷; “keep me logged in” habits become an unlocked entry point to accounts
- » **Increasing pool for fraudster opportunity** as more people conduct mobile transactions

Cross Border

- » **Uncertainties, blind spots and new payment methods;** it becomes difficult to determine transaction origination; lack of verifiable data on consumers (particularly with GDPR)

Digital

- » **Fast transaction;** digital goods/ services, such as downloads and subscriptions, tend to occur quickly; lack of a physical delivery address eliminates buffer period for fraud verification before shipment; with fear of abandonment, merchants struggle with balancing fraud prevention and minimising customer friction.
- » **Favourite target for fraudster card testing;** use of bots to test stolen credit card information with lower value goods/services (typical of digital goods/services) tend to arouse less suspicion.
- » **Easy targets;** synthetic identities and stolen data make it difficult to distinguish between malicious attacks and legitimate customers in the anonymous channel.



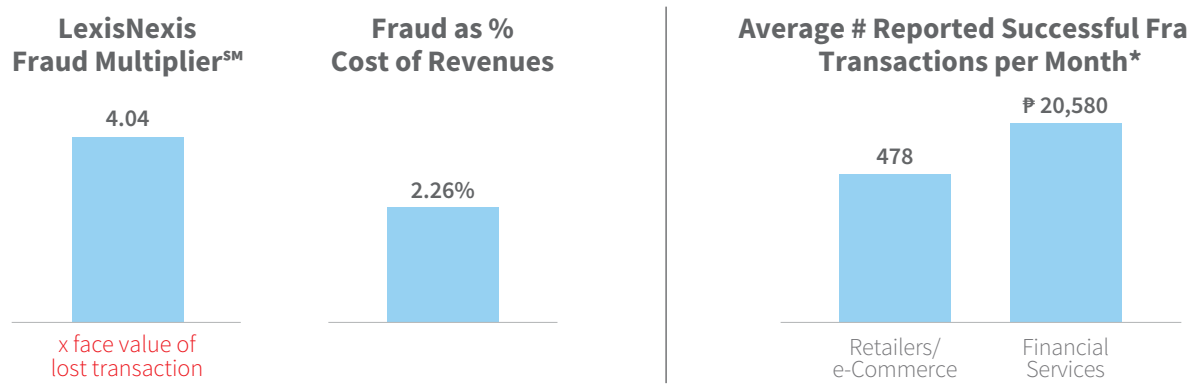
16 ThreatMetrix® H2 2018 Cybercrime Report
17 4 Mobile Fraud Trends to Look for in 2019; <https://threatmetrix.com/digital-identity-blog/fraud-prevention/4-mobile-fraud-trends-look-out-for-2019>



This results in higher volumes and cost of fraud for businesses that offer m-Commerce.

- » Every **fraudulent transaction** actually costs these businesses **4.04 times the value of lost transaction**. This is higher than the average across organisations (3.46) overall.
- » This channel also experiences a higher number of successful fraud transactions that involve higher average values.

Among Businesses Offering m-Commerce



* Based on self-reported numbers and likely recall; not meant to be exact; may increase or decrease based on seasonality

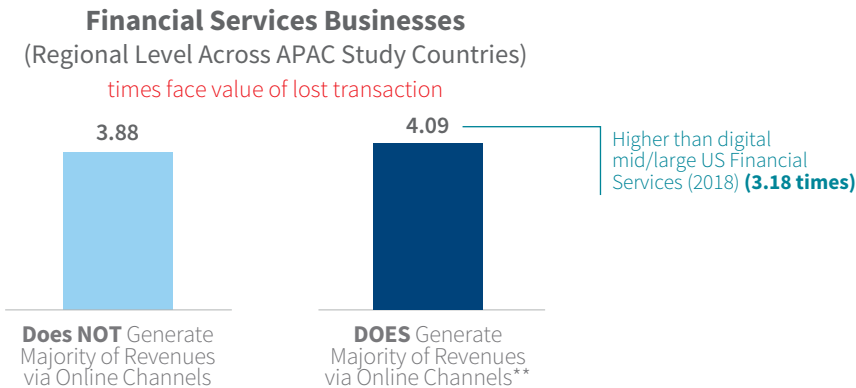
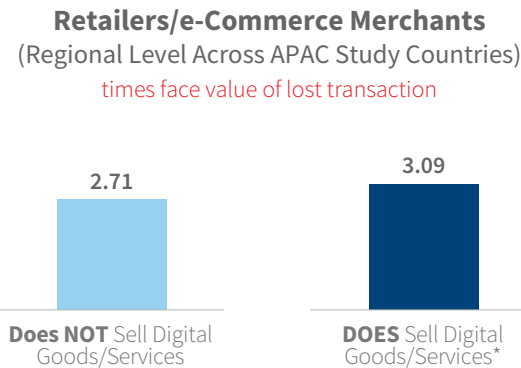




Regionally, those that are “digital” have even higher risks and costs associated with fraud, which tends to overlap with m-Commerce.

- » For digital Retailers, e-Commerce merchants, and Financial Services businesses, identity verification becomes a challenge and a risk.
 - » For Retailers/e-Commerce merchants, speed and type of transaction are the issue. Digital goods/services involve more immediacy of distribution/downloading; whereas merchants that sell physical goods have a delivery address for shipping and a buffer time between transaction and shipment to confirm identity and legitimacy of the sale, this is not the case for those selling digital goods. There is more real-time need for fraud detection efforts.
 - » For Financial Services businesses, the anonymity of the online channels makes identity verification much more difficult.
 - » And, with all segments, devices (computers, tablets, mobile phones) can confuse things with spoofing and malware.
- » Across industries, those that are digital get hit with a higher cost of fraud.

LexisNexis Fraud MultiplierSM



*sells goods/services that are stored, delivered, and used in electronic format, including cloud-based applications, digital services, digital subscriptions, downloadable software, eBooks, eLearning/online courses, eGift cards, electronic tickets, media streaming/ downloads, mobile apps, online games/gaming, photos/graphics

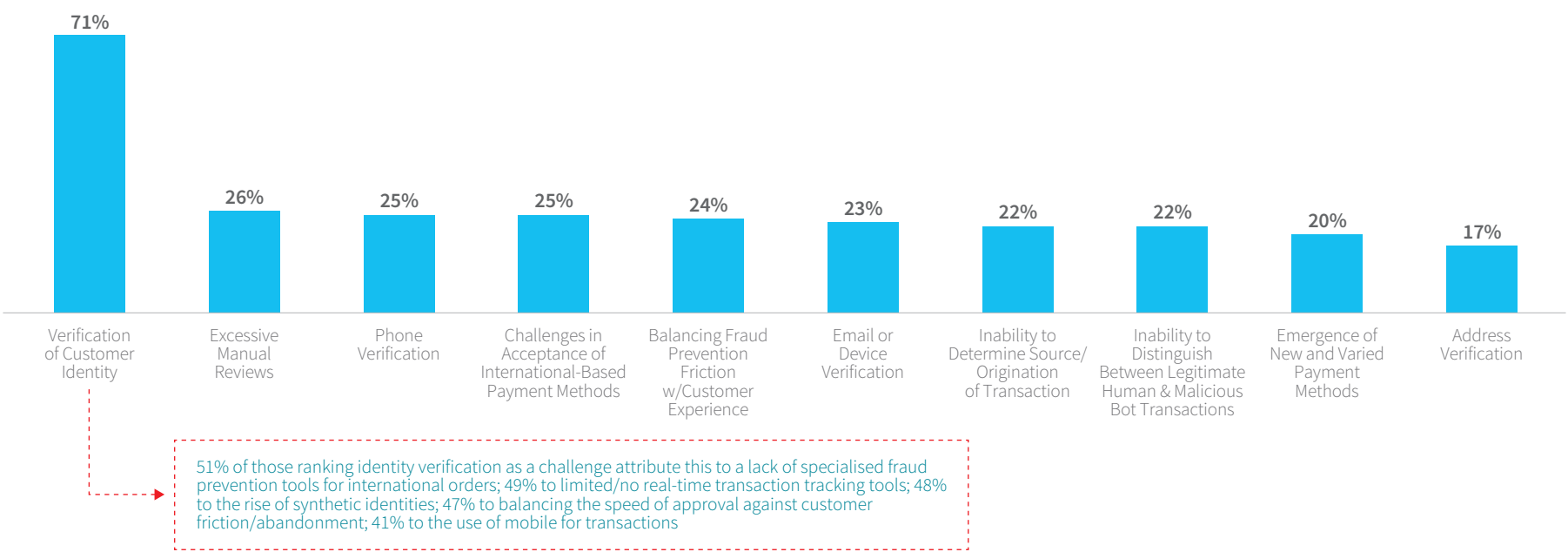
**earn 50% or more of revenues through online channels



Regionally, risk verification is the most common concern for Omni-Retailers and e-Commerce merchants that sell digital goods/services.

» Various factors contribute to difficulties with customer identity verification, including lack of specialised fraud prevention tools for international orders or for real-time tracking, the rise of synthetic identities, balancing the speed of approval against customer friction, and the use of mobile (where attack rates are on this rise).

Top 3 Challenges Related to Selling Digital Goods & Services
(Regional Level Findings For Omni-Retailers and e-Commerce Merchants Across APAC Study Countries)



5 Businesses are not effectively fighting fraud.



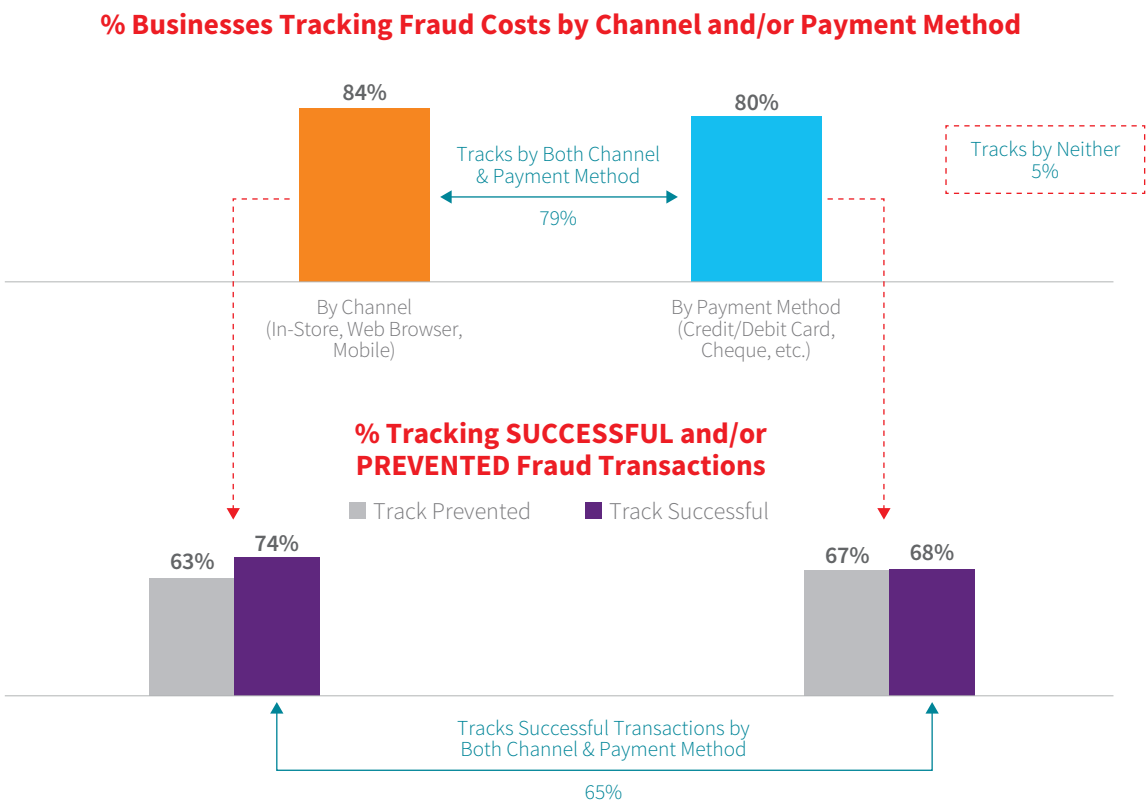
- Research Definitions
- Key Findings
- Recommendations
- Summary





A majority report that they track fraud costs by channel and payment method.

- » However, only 65% appear to be tracking *successful* fraud transactions by both channel and payment method.
- » Not tracking successful and prevented fraud transactions by both channel and payment method leaves businesses vulnerable to fraudsters, particularly within the online and mobile channels, where fraudsters are adept at testing for weaknesses.



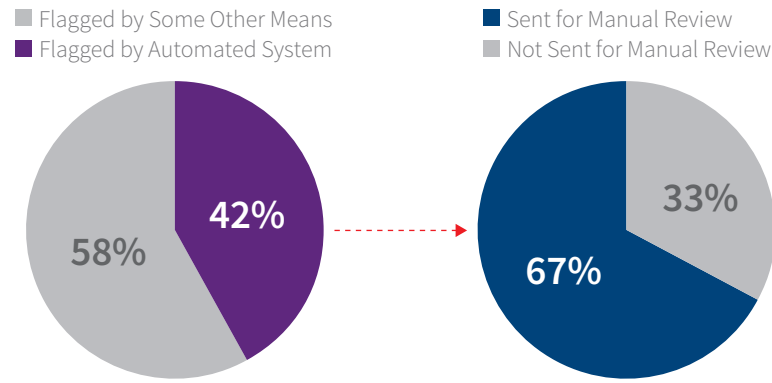


Only 42% of transactions are flagged by an automated system.

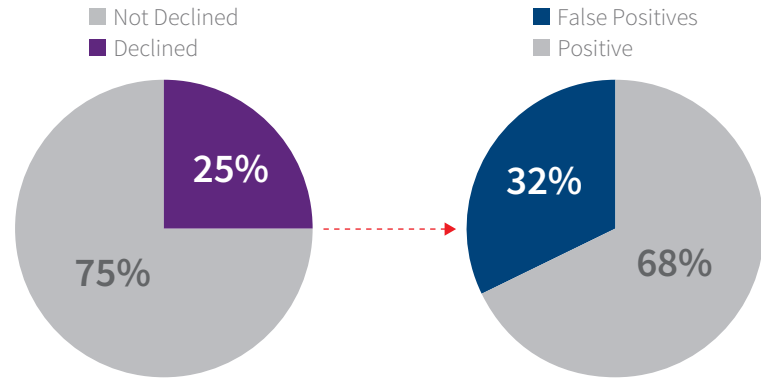


- » And among those that are, 67% are sent for manual review.
- » And manual reviews aren't preventing false positives. 32% of declined transactions turn out to be false positives. This has cost and revenue implications, as well as longer-term customer relationship consequences.

% Transactions Flagged by Auto System. Sent for Manual Review



% Flagged Transactions That Are Declined. False Positives





Research
Definitions



Key Findings



Recommendations



Summary



⑥ The use of more advanced fraud mitigation solutions is limited.





Research Definitions



Key Findings



Recommendations



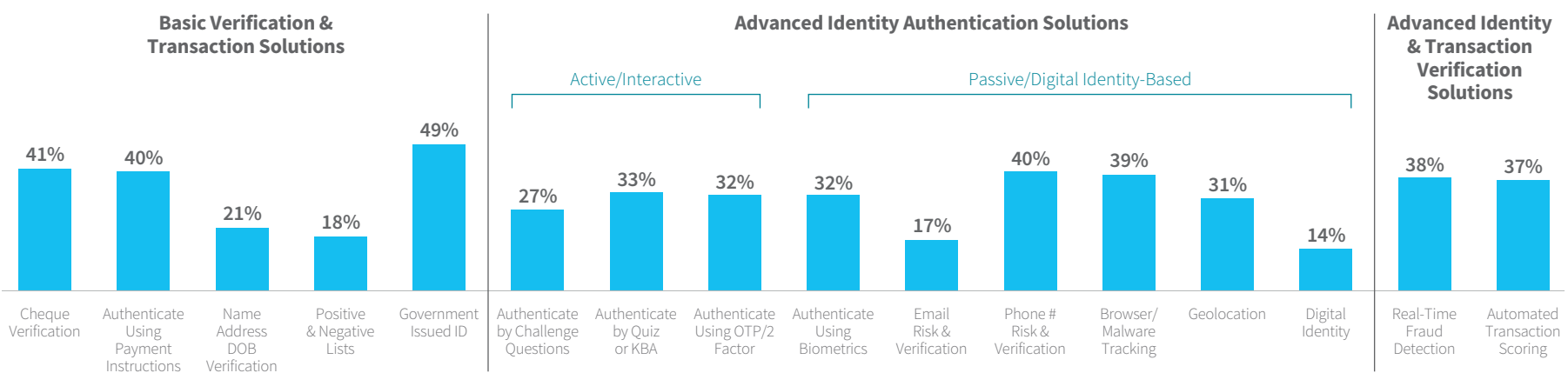
Summary



An average of 5.1 fraud mitigation solutions are being used across the surveyed industries.

- » However, the use of more sophisticated solutions to address the emerging multi-faceted nature of fraud is limited, particularly with regard to behavioural biometrics and other digital identity solutions that can fight synthetic identity fraud and botnet attacks. Given similar incidence rates between some of the physical (cheque verification, government issued ID) and digital solutions (real-time fraud detection, automated scoring), this suggests some layering of solutions for more effective fraud detection. However, there is still a significant portion of merchants/businesses who are not doing so.
- » The use of solutions to address mobile threats (digital identity, geolocation, OTP/2 factor) is limited. And whilst solutions are a sizeable portion of fraud mitigation budgets, manual reviews are still nearly one-fifth of costs, further suggesting that current fraud prevention attempts are lacking.

Fraud Mitigation Solutions Use (Avg. 5.1 Solutions Used)



Distribution of Fraud Mitigation Costs by Percent of Spend

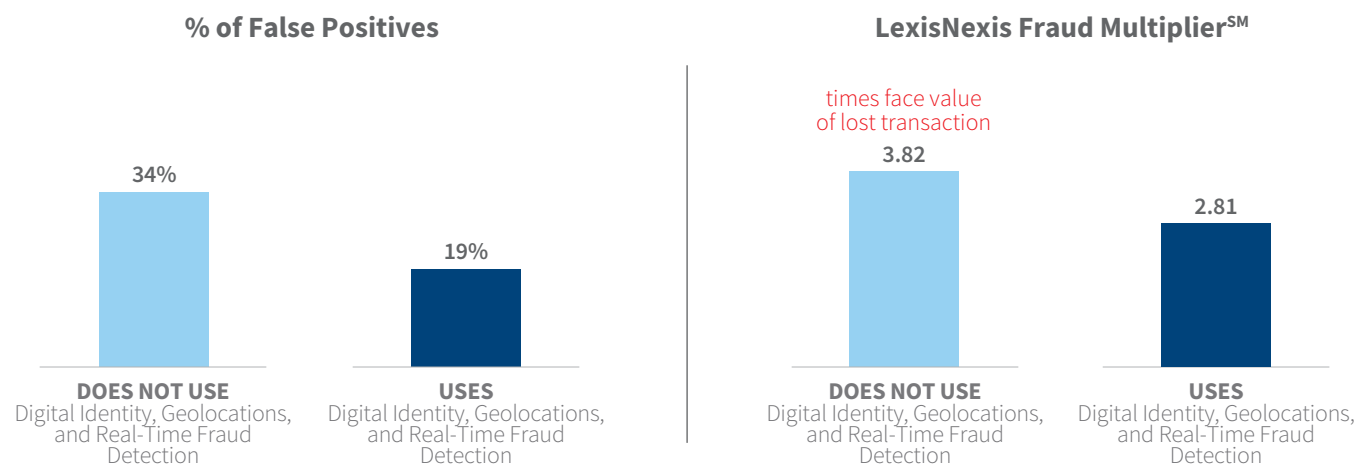




But it’s not just about the number of solutions. It’s important to layer the right combination to meet threats from specific types of channels and transactions.

- » Bundling Digital Identity, Geolocation, and Real-Time Fraud Detection solutions can be an effective fraud mitigation tool.
- » Regional findings show that APAC businesses in surveyed industries that do this are better able to address mobile threats and the fast-paced challenge of digital/anonymous transactions, resulting in fewer successful fraudulent transactions and lower fraud costs overall.

Businesses That Allow Mobile Transactions
(Regional Level Findings in Surveyed Industries Across APAC Study Countries)





Research Definitions



Key Findings



Recommendations



Summary



Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria as well as both identity and transaction risk.



Fraud Issues

Digital Goods & Services: fast transactions, easy synthetic identity and botnet targets; need velocity checking to determine transaction risk along with data and analytics to authenticate the individual

Account-related fraud: breached data requires more levels of security, as well as authenticating the person from a bot or synthetic ID

Synthetic identities: need to authenticate the whole individual behind the transaction in order to distinguish from fake identity based on partial real data

Botnet attacks: mass human or automated attacks often to test cards, passwords/credentials or infect devices

Mobile channel: source origination and infected devices add risk; mobile bots and malicious malware makes authentication difficult; need to assess the device and the individual

Solution Options

Assessing the transaction risk

Velocity checks / transaction scoring: monitors historical shopping patterns of an individual against their current purchases to detect if the number of orders by the cardholder match up or if there appears to be an irregularity (*Solution examples: real-time transaction scoring; automated transaction scoring*)

Authenticating the physical person

Basic Verification verifying name, address, DOB or providing a CVV code associated with a card (*Solution examples: cheque verification services; payment instrument authentication; name/address/DOB verification*)

Active ID Authentication use of personal data known to the customer for authentication; or where user provides two different authentication factors to verify themselves (*Solution examples: authentication by challenge or quiz; authentication using OTP / 2 factor*)

Authenticating the digital person

Digital identity / behavioural biometrics: analyses human-device interactions and behavioural patterns such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognising normal user and fraudster behaviour (*Solution examples: authentication by biometrics; e-mail/phone risk assessment; browser/malware tracking; device ID / fingerprinting*)

Device assessment: uniquely identify a remote computing device or user (*Solution examples: device ID / fingerprint; geolocation*)



Research
Definitions

Key Findings

Recommendations

Summary

Technology is the Key

- » To minimize fraud, organizations can no longer rely on manual processes with the assistance of limited technologies to reduce challenge rates, manual reviews, and costs.
- » Businesses need a robust fraud and security technology platform that helps them adapt to a changing digital environment, offering strong fraud management and resulting in a frictionless experience for genuine customers.
- » Deploying technologies, which can recognize customers, pinpoint fraud, and build the fraud knowledge base to streamline onboarding, can prevent account takeovers and detect insider threats.
- » Using valuable data attributes like users' login from multiple devices, locations, and channels is essential for identifying risks.
- » Enabling integrated forensics, case management, and business intelligence can help to improve productivity.





- Research Definitions
- Key Findings
- Recommendations
- Summary

Multi-Layered Fraud Defense is Required

- » Single point protection is no longer enough and results in single point of failure.
- » As consumers transact across locations, devices, and geographies, user behaviors, such as transaction patterns, payment amounts, and payment beneficiaries, are becoming more varied and less predictable.
- » A multi-layered, strong authentication defense approach is needed. This includes a single authentication decision platform that incorporates real-time event data, third-party signals, and global, cross-channel intelligence.
- » Also required is the ability to examine malware level threats, Bot, and remote access Trojan and IP spoofing detection across web and mobile channels.
- » At the same time, the ability to provide behavioral analytics and reduce false positives and customer friction is key.





Research
Definitions



Key Findings



Recommendations



Summary



Improve Decisioning With Machine Learning

- » Employing machine technology will further reduce fraud mitigation costs and manpower by adapting to changing customer behaviors over time.
- » Organisations that have existing fraud detection policies can test different machine learning models until they find one that best aligns with their business objectives.
- » Such a model can deliver benefits that include enhanced fraud detection, reduction in false positives, improved identification of trusted customers, and optimized challenge and maximum review rates.





Recommendations

-  Research Definitions
-  Key Findings
-  Recommendations
-  Summary
- 

Research
Definitions

Key Findings

Recommendations

Summary

Creating an Industry Alliance is a Great Option

- » Organisations are likely fighting against the same group of fraudsters. In fact, fraud patterns and risks share many similarities across industries and geographies.
- » Building an industry-specific alliance that exchanges important information can keep members up-to-speed on industry fraud patterns and tactics, complimenting their own intelligence, and allowing them to more accurately identify and track at-risk individuals and devices. Such information can include:
 - » Historic blacklisted devices
 - » Mule accounts and associated fraud strategies
 - » Specific risks pertaining to industry/use case/geography





Research
Definitions



Key Findings



Recommendations



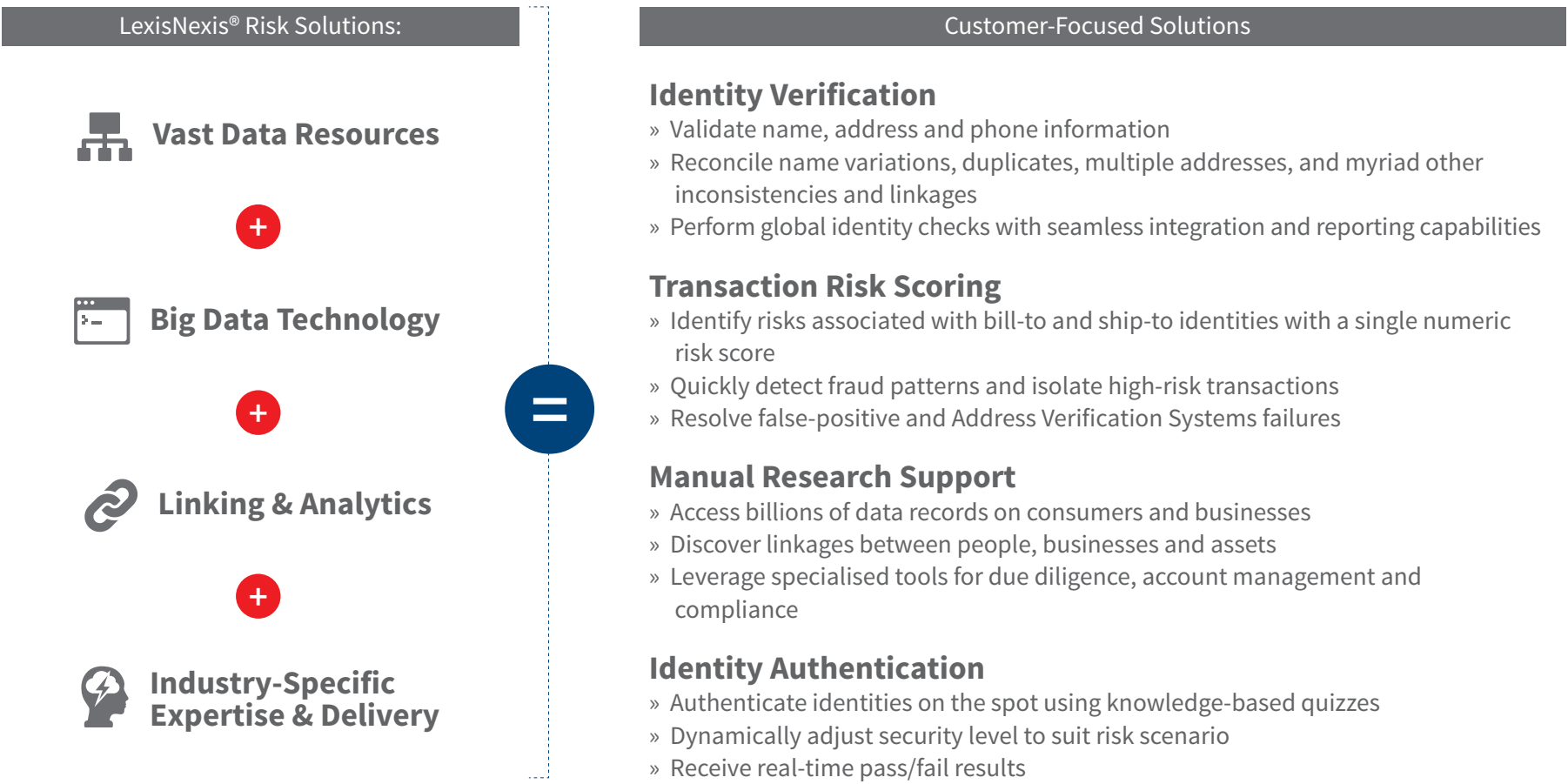
Summary



LexisNexis® Risk Solutions can help



LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud.



For more information: visit <https://risk.lexisnexis.com/global/en/financial-services/fraud-and-identity-management>



Regional Summary. Fraud is sizeable across APAC businesses, but is more pronounced for the Financial Services industry, as well as businesses of all types that conduct transactions through the mobile channel.

- » These businesses experience high successful fraud volumes and transactions amounts, even though they are using just as many fraud mitigation solutions, on average, than others.
- » Financial Services businesses also attribute more fraud losses to identity fraud and are more likely to rank identity verification as a challenge than other businesses.

	Region Overall	Industry			Offer m-Commerce	
		Retail	e-Commerce	Financial Services	Yes	No
LexisNexis Fraud Multiplier SM	3.40	2.80	3.00	3.92	3.99	2.92
Fraud Costs as % of Revenues	1.75%	1.64%	2.50%	1.56%	1.96%	1.65%
Avg. # Fraud Mitigation Solutions	5.5	5.5	5.4	5.5	5.5	5.4
Avg. # SUCCESSFUL Monthly Fraud Transactions	391	305	270	480	564	191
Avg. \$ Amount of SUCCESSFUL Monthly Fraud Transactions	₱21,535	₱17,476	₱18,040	₱25,068	₱26,910	₱15,296
% of m-Commerce That Offer Mobile Apps	95%	93%	97%	95%	95%	
% Distribution of Losses Related to Identity Fraud	33% (14% synthetic)	27% (9% synthetic)	29% (13% synthetic)	38% (16% synthetic)	34% (15% synthetic)	32% (13% synthetic)
% Ranking Identity Verification as a Top Online/Mobile Challenge	65%	58%	61%	70%	64%	66%



Research Definitions



Key Findings



Recommendations



Summary



And when looking *within* industries, it is digital goods merchants and digital Financial Services businesses that get hit hardest by fraud.

- » Digital goods account for nearly half of Retail/e-Commerce fraud losses, whilst the online/mobile channels account for nearly two-thirds of Financial Services fraud losses.
- » These businesses have higher successful fraud volumes and values than others, which contributes to higher fraud costs.
- » Businesses that are digital in nature (either by type of good sold or transaction channel) are highly likely to allow transactions through high-risk mobile apps, which further compounds the challenges faced regarding identity verification, including synthetic identities.

	Retail/e-Commerce		Financial Services	
	Sell digital goods*	Sell physical goods only	Digital**	Non-digital
LexisNexis Fraud Multiplier SM	3.09	2.71	4.09	3.88
Fraud Costs as % of Revenues	2.45%	1.56%	2.38%	1.31%
% Fraud Losses From...	Digital goods = 39%		Online/mobile channels = 62%	Online/mobile channels = 48%
Avg. # Fraud Mitigation Solutions	5.8	5.2	5.4	5.5
Avg. # SUCCESSFUL Monthly Fraud Transactions	443	156	832	360
Avg. \$ Amount of SUCCESSFUL Monthly Fraud Transactions	₱20,708	₱14,770	₱52,917	₱15,710
% of m-Commerce That Offer Mobile Apps	98%	88%	94%	96%
% Distribution of Losses Related to Identity Fraud	31% (13% synthetic)	25% (8% synthetic)	38% (16% synthetic)	38% (17% synthetic)
% Ranking Identity Verification as a Top Online/Mobile Challenge	60%	59%	75%	57%
% Ranking Synthetic Identities as Top Challenge to Identity Verification	48%			



Fraud is also sizeable across APAC countries.



Research Definitions



Key Findings



Recommendations



Summary



	Region Overall	Country			
		Singapore	Indonesia	Malaysia	Philippines
LexisNexis Fraud Multiplier SM	3.40	3.45	3.25	3.57	3.46
Fraud Costs as % of Revenues	1.75%	1.57%	1.66%	1.93%	2.03%
Avg. # Fraud Mitigation Solutions	5.5	5.4	5.6	5.6	5.1
Avg. # SUCCESSFUL Monthly Fraud Transactions	391	317	464	401	332
Avg. \$ Amount of SUCCESSFUL Monthly Fraud Transactions	₱21,535	₱21,873	₱22,136	₱23,452	₱18,453
% of m-Commerce That Offer Mobile Apps	95%	92%	98%	93%	94%
% Distribution of Losses Related to Identity Fraud	33% (14% synthetic)	34% (14% synthetic)	34% (13% synthetic)	31% (15% synthetic)	34% (14% synthetic)
% Ranking Identity Verification as a Top Online/Mobile Challenge	65%	65%	62%	68%	65%



For more information: visit

<https://risk.lexisnexis.com/global/en/financial-services/fraud-and-identity-management>

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., used under license. LexisNexis Fraud Multiplier is a service mark of RELX Inc. True Cost of Fraud is a service mark of LexisNexis Risk Solutions Inc. Copyright © 2019 LexisNexis. NXR12136-00-0519-EN-US

