LexisNexis®
RISK SOLUTIONS

TRUE COST OF FRAUD APAC STUDY

REGIONAL REPORT

JULY 2022

BACKGROUND & METHODOLOGY

The LexisNexis® Risk Solutions True Cost of Fraud™ Study helps companies grow their business safely by navigating the growing risk of fraud.

The research provides a snapshot of:

- Current fraud trends in the APAC retail, ecommerce, financial services and lending markets.
- Key pain points related to adding new payment mechanisms, transacting through online and mobile channels and expanding internationally.

COVID-19 Impact:

- Data collection occurred during February/March 2022; many of the survey questions reference the past 12 months; therefore, findings reflect activity, fraud risks, challenges and costs that have been impacted by COVID-19 fears, changing behaviors and forced lockdowns.

Fraud Definitions:

- Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information
- Fraudulent requests for refunds/returns, bounced checks
- Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items
- Fraudulent applications (e.g., purposely providing incorrect information about oneself, such as income, employment, etc.)
- Account takeover by unauthorized persons
- Use of accounts for money laundering

This research covers consumer-facing fraud methods:

- Does not include insider fraud or employee fraud

The LexisNexis Fraud Multiplier™ cost:

- Estimates the additional costs incurred beyond the actual monetary loss for a fraudulent transaction. This is expressed as a multiplier based on the lost monetary value and additional costs involving fees, fines, labor investigation, merchandise replacements and external support with investigations and recovery.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

BACKGROUND & METHODOLOGY

The study is a comprehensive survey of 387 risk and fraud executives in Retail, Ecommerce and Financial Services/Lending in the APAC region.

	Malaysia	Philippines	Singapore	Thailand	Overall
Retail	30	42	47	38	38
Ecommerce	30	33	31	31	31
Financial Services	30	33	30	30	30
Buy Now, Pay Later/Digital Wallets	30				20
Digital Bank/Alternative Lending	120				5
Mobile Trading	30				5
				TOTAL	387

Surveyed industries include*:

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

Ecommerce
Earn 80% or more of revenues through online channels

Financial Services
Asset Management
Banking/Mortgage
Consumer Lending
Financial Planning

New Industries
Buy Now, Pay Later
Digital Wallets
Digital Bank
Alternative Lending
Mobile Trading

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

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

KEY FINDINGS

01 **The cost of fraud for surveyed industries in APAC has risen sharply.** On average, a fraudulent transaction costs nearly four times the lost transaction value on average now, compared to between 3.46 to 3.57 times from 3 years ago. While retail and ecommerce industries are being hit with fraud, financial institutions are getting hit harder in terms of targeted scams, attack volume and costs.

02 **Consumer and merchant behaviors have changed with the acceleration of the digital transformation,** including increased adoption of remote channel use, digital payment methods and omnichannel focus. While digital channels have expanded, in-person transactions are still very prevalent. For example, Buy Online/Pick Up in Store (BOPIS) is on the rise and some ecommerce merchants have expanded to an omnichannel strategy (clicks-to-bricks) involving physical stores or partnership with retailers.

03 **The digital transformation is presenting opportunities for fraudsters, contributing to the increased in fraud costs.** Fraud losses continue to grow as the adoption of mobile apps and digital wallets, along with other contactless payment methods, has accelerated in recent years. Buy Now, Pay Later (BNPL) services account for over one-tenth of payment method losses, which is disproportionately higher than the average volume of transactions through these apps. While merchants and financial institutions focus on fraud at the point of sale/distribution of funds, they need to also focus on the account login and other use cases in the customer journey.

04 **Identity verification is a common top challenge across the customer journey, particularly at the new account creation and login stages.** But it is also important to assess the payment risk as well. Fraud can occur along the entire customer journey, such as user authentication, new account creation, logins and payments.

05 **Merchants and financial services firms can reduce fraud costs and risks** through the implementation of a holistic approach by bringing together vital elements in cybersecurity, digital customer experience and fraud operations through a multi-layered solution approach.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 01

KEY FINDING 01

The cost of fraud for surveyed industries in APAC has risen sharply. Every fraudulent transaction costs nearly four times the lost transaction value on average now, compared to between 3.45 and 3.57 times 3 years ago.

The cost of fraud is for financial services institutions, which generally involves significant internal and external resources in remediation efforts, given the need to recoup/repay fraud losses where customer accounts have been compromised.

While fraud volume is up across organizations, financial institutions are battling significantly higher levels than before the pandemic. This comes at a time of increased online and mobile transactions given the digital transformation and a spate of SMS/phishing scams targeting customer identity information and account access details.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 01

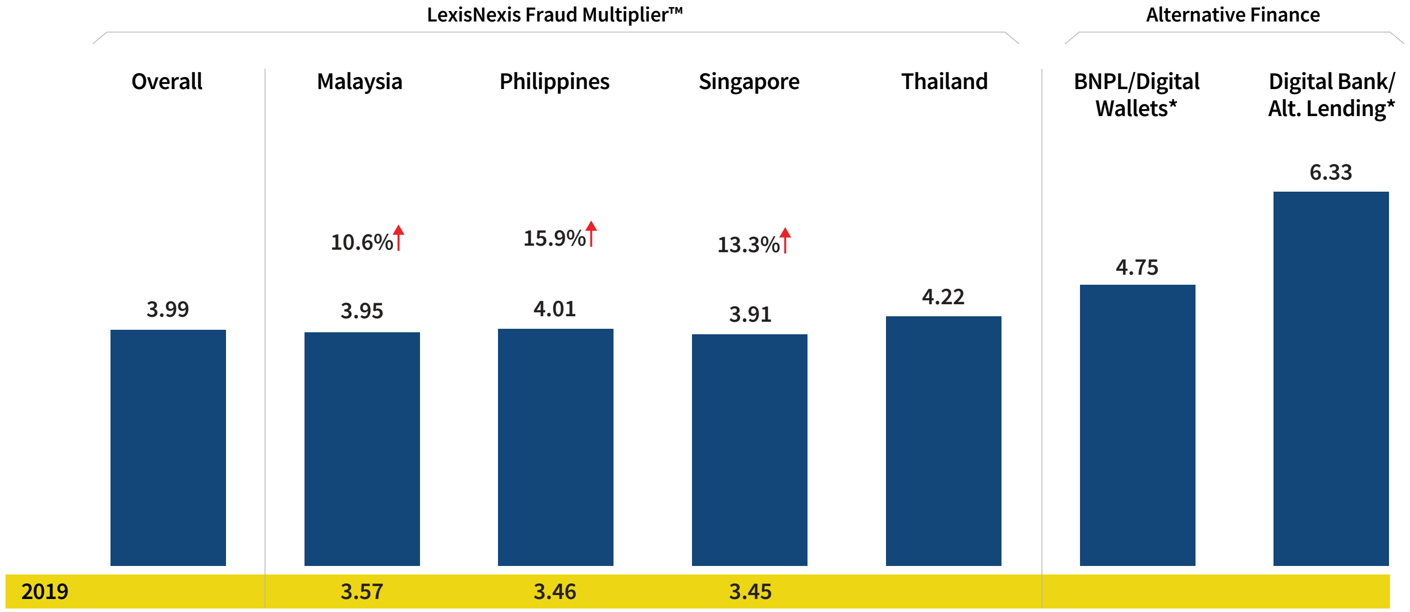
FRAUD COSTS & VOLUME

The cost of fraud has risen sharply for APAC merchants and financial institutions.

For every fraudulent transaction, the cost to APAC businesses is nearly four times (3.99) the amount of the lost transaction value. For firms tracking from just before the COVID-19 pandemic (3 years ago), this represents a 10% - 16% rise depending on the market. The Fraud Multiplier™ tracks closely to the Indian and Japanese markets surveyed in 2021, particularly where there has been a rash of financial digital banking scams.

Financial institutions tend to have a higher fraud multiplier; given the heavy account-based nature of their business and need to repay/recoup fraud to customer accounts, they often employ more internal and external labour for investigation, detection and recovery.

Cost of Fraud: LexisNexis Fraud Multiplier™



Fraud Multiplier™ Comparisons

2022 APAC Markets

Financial Services/Lending (5.24)
Ecommerce (3.56)
Retail (3.51)

2021 APAC Markets

Australia (3.51)
Hong Kong (3.61)
India (3.84)
Japan (3.87)

Survey Questions:
Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.
Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

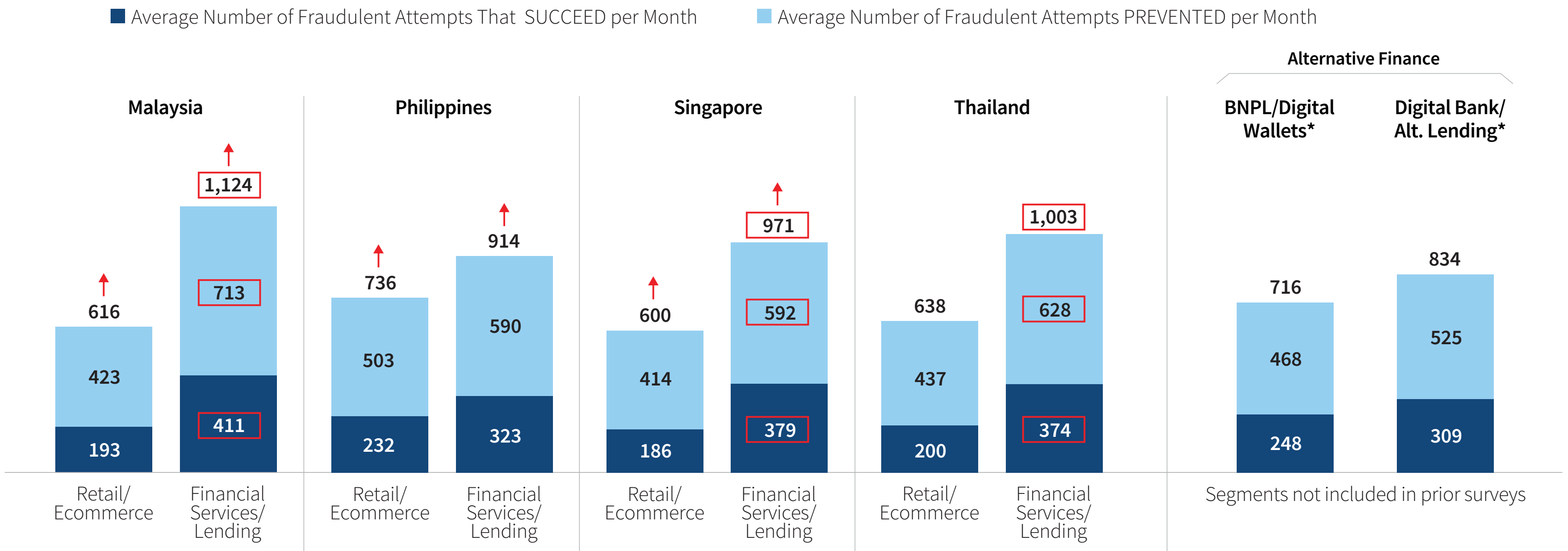
KEY FINDING 01

FRAUD COSTS & VOLUME

APAC merchants and financial institutions are battling significantly more fraud attacks than before the COVID-19 pandemic, with a need for digital identity solutions.

Financial institutions have experienced the sharpest increases. Online banking in the Philippines has spiked since the start of the pandemic, with digital fraud attempts increasing by over 50% during the past year.[1] Further, there have been a spate of SMS and phishing scams targeting customers of APAC banks, including interception of one-time passwords and fake messages in the same thread as legitimate text messages previously sent by a bank.[2,3,4] Where fraudsters obtain real customer passwords and identity information, financial institutions will be challenged to distinguish between legitimate and fraudulent transactions unless there is use of solutions that detect anomalous digital behaviors that don't align with real customers' typical online or mobile channel activities.

Average Monthly Fraud Attacks



2019 Prevented	130	195	138	223	64	250	**Thailand not included in prior surveys**
2019 Succesful	157	338	143	203	86	180	

↑= significantly or directionally higher than 2019 ☐ = significantly or directionally higher than other segment within country

Q22/24: In a typical month, approximately how many fraudulent transactions are prevented by/successfully completed at your company?

1 https://gulfnews.com/business/philippines-short-list-of-top-financial-scams-central-bank-cracks-the-whip-on-fraud-money-laundering-1.1639325591494?slide=3
2 https://www.globalcompliancenews.com/2022/02/19/singapore-authorities-introduce-measures-to-combat-sms-phishing-scams280122/
3 Https://www.bangkokpost.com/business/2196191/central-bank-issues-warning-over-online-financial-scams
4 https://www.malaymail.com/news/opinion/2022/01/23/scams-and-banks/2036945

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

KEY FINDING 02

KEY FINDING 02

Consumer and merchant behaviors have changed with the acceleration of the digital transformation, including more remote channel use, more digital payment methods and more omnichannel focus.

The shift towards online and mobile channels was well underway even before the pandemic. But transactions and activities from traditional channels remain sizeable; this can include Buy Online/Pick Up in Store (BOPIS) as well as where ecommerce merchants are expanding an omnichannel presence through their own physical stores or in partnership with retailers for delivery.

Transaction volumes through digital/mobile wallets have increased, and this trend is a reflection of changing consumer behaviour and faster adoption of digital payment options. Just under half of the retailers in the survey offer Buy Now, Pay Later (BNPL), as the volumes of these transactions continue to increase. There are expectations that the BNPL volumes will grow significantly by 2025 (FIS Worldpay, The Global Payments Report 2022).

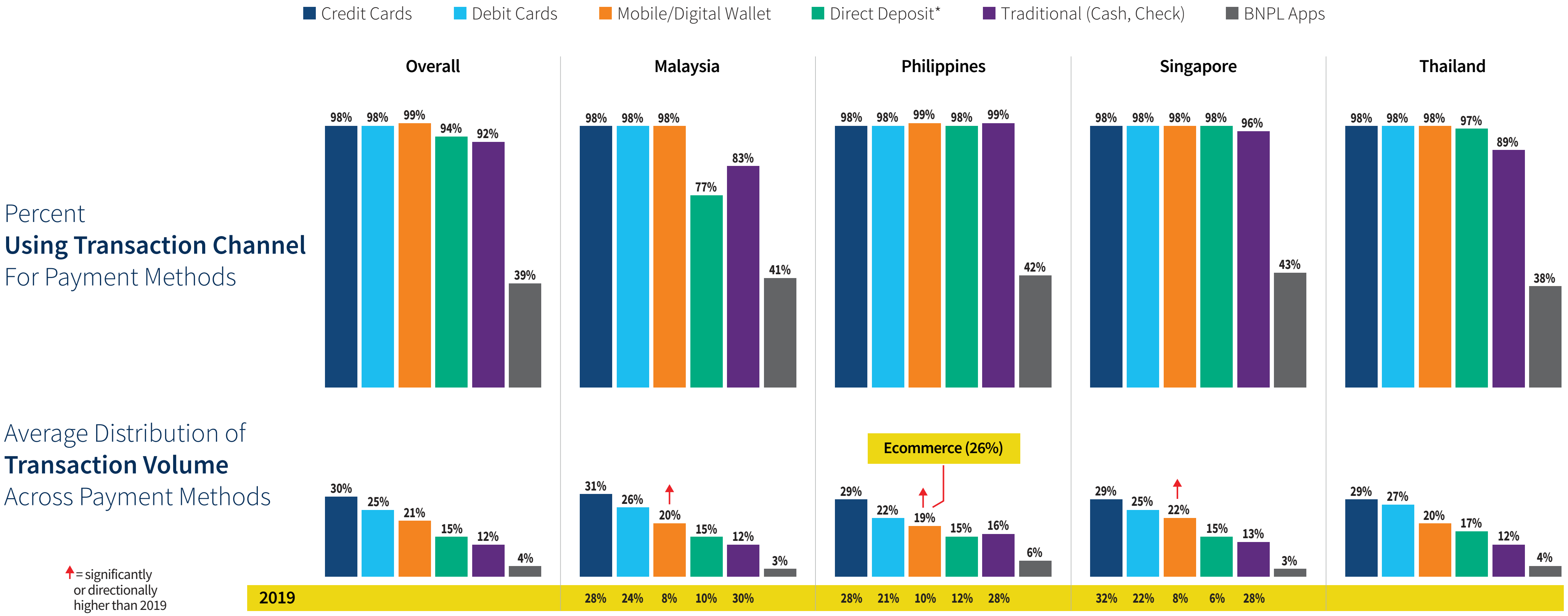
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02
TRANSACTIONAL TRENDS

The volume of transactions through mobile and digital wallets has increased in markets trending from 3 years ago. BNPL is offered by just under half of merchants/FIs, though the *reported* volume of transactions through these apps is still emerging.

As the pandemic drove transactions to online and mobile channels, the volume involving cash has dropped as mobile and digital wallets has increased to a level similar to that of debit and credit cards, particularly with Filipino ecommerce merchants. APAC consumers have changed the way that they shop and pay, with many being exposed to – and embracing of – new payment methods such as digital wallets, BNPL apps, QR codes and even cryptocurrency.[5] They provide a means to expand financial inclusion for the unbanked and underbanked populations.

The volume of transactional share for mobile and digital wallets, real-time payments and Buy Now, Pay Later is expected to grow by 2025 across the study countries.[6]



Survey Questions:
Q3: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment methods currently accepted by your company.

---

[5] https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2021/may/pandemic-alters-spending-habits-in-apac-drives-rapid-shift-to-emerging-payment-technologies/
[6] FIS Worldpay, The Global Payments Report 2022; https://worldpay.globalpaymentsreport.com/en

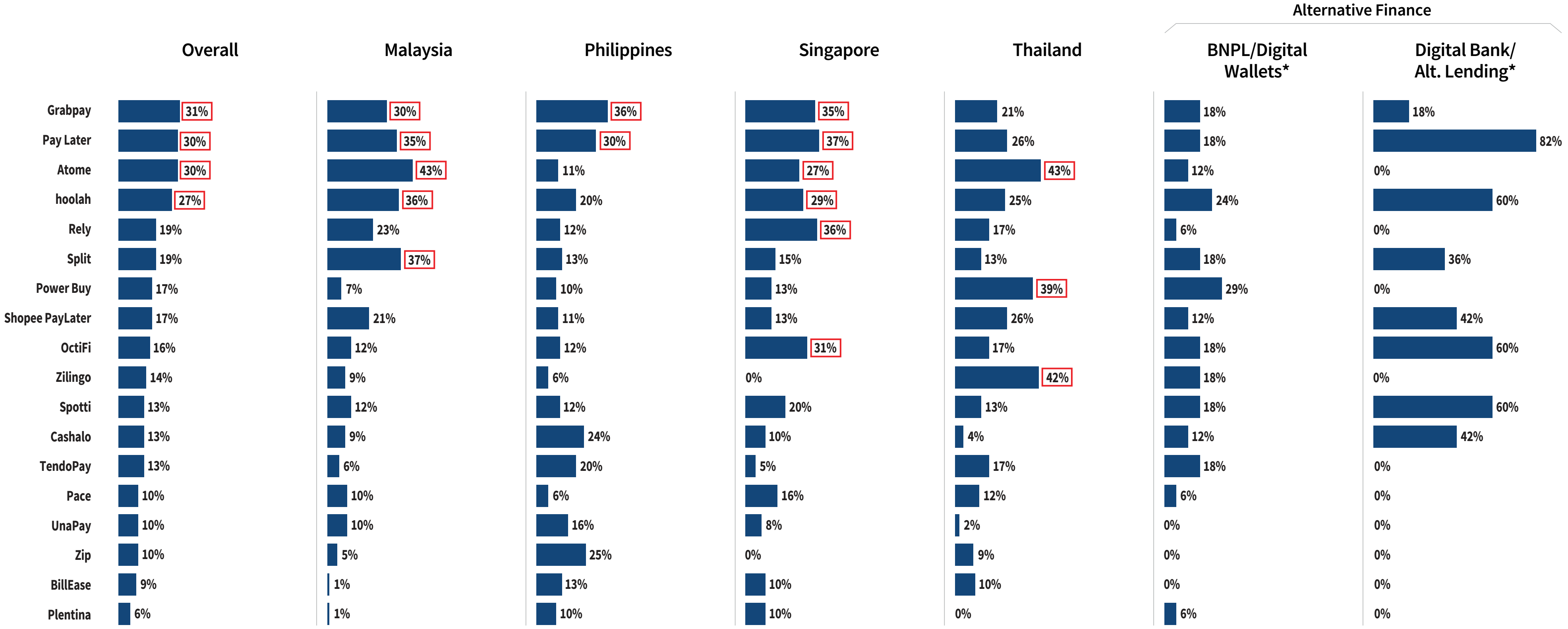
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02

BUY NOW, PAY LATER PROVIDER TRENDS

The BNPL market is competitive across many providers, particularly in Malaysia and Singapore. It is more fragmented in the Philippines and Thailand.

Buy Now, Pay Later Provider Use



Other (mentioned more than once): Affirm, NETSPay, FavePay, Lazada, IOUpay

🟥 = significantly or directionally higher than most or all other providers within segment/country

Survey Questions:
Q3b: (ASK IF 3_7 >0) Which Buy Now, Pay Later providers do you allow for payment transactions?

*Caution: small sample sizes of N=17 and N=5, respectively (no sig. testing)

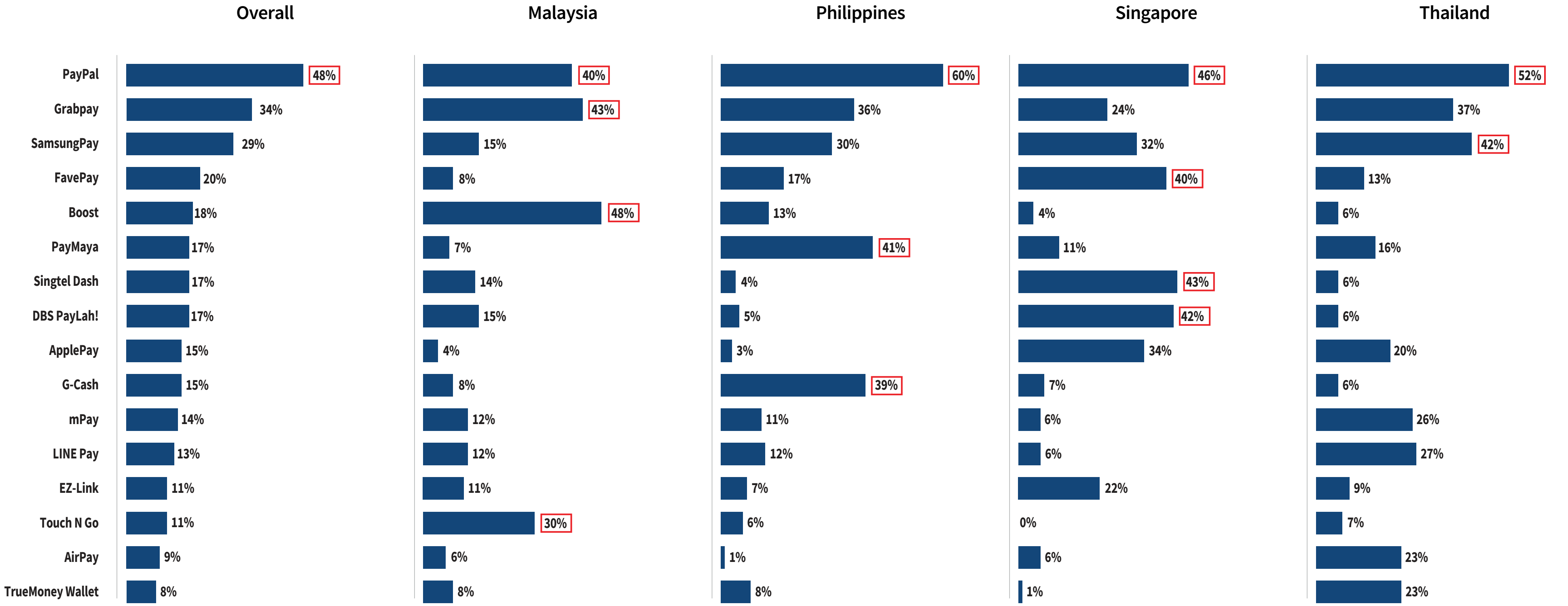
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02

MOBILE AND DIGITAL WALLETS PROVIDER TRENDS

The mobile and digital wallets market is dominated by a few providers. Whilst PayPal is a leader across markets, the other top providers vary by country.

Mobile and Digital Wallets Provider Use



Other (mentioned more than once): Coins PH, WeChat Pay, Trust Wallet, AliPay, Moneygment, BigPay, ML Wallet, AEON Wallet, Lazada Wallet, mPay, Dragon Pay

☐ = significantly or directionally higher than most or all other providers within segment/country

Survey Questions:
Q3b: (ASK IF 3_7 >0) Which Buy Now, Pay Later providers do you allow for payment transactions?

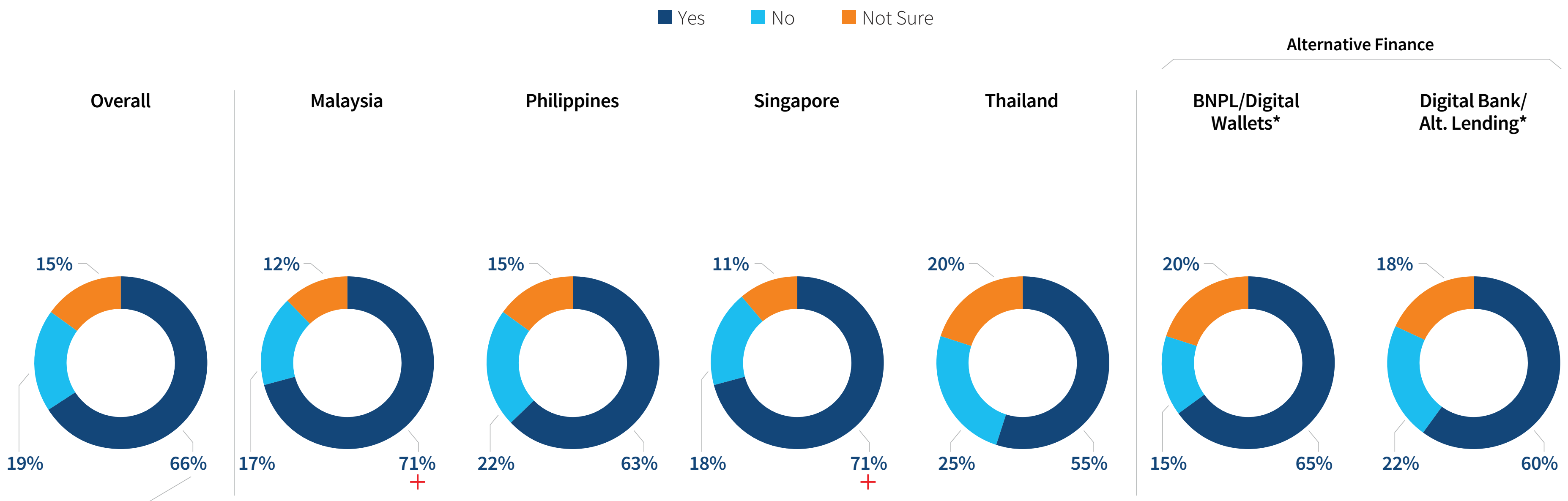
*Caution: small sample sizes of N=17 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02
TRANSACTIONAL TRENDS

The digital transformation has generated an increase in new accounts and digital payments during the past 12 months, primarily among ecommerce and financial services/lending firms.

Increase in Account Creations/Digital Payments Last 12 Months Given the Digital Transformation



Retail = 55%
Ecommerce = 73%
Financial Services/Lending = 68%

+ = significantly or directionally higher than all or most other markets/segments

Survey Questions:
Q34: With regard to digital transformation, has there been an increase in account creations/payments over the past 12 months?

*Caution: small sample sizes of N=17 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02

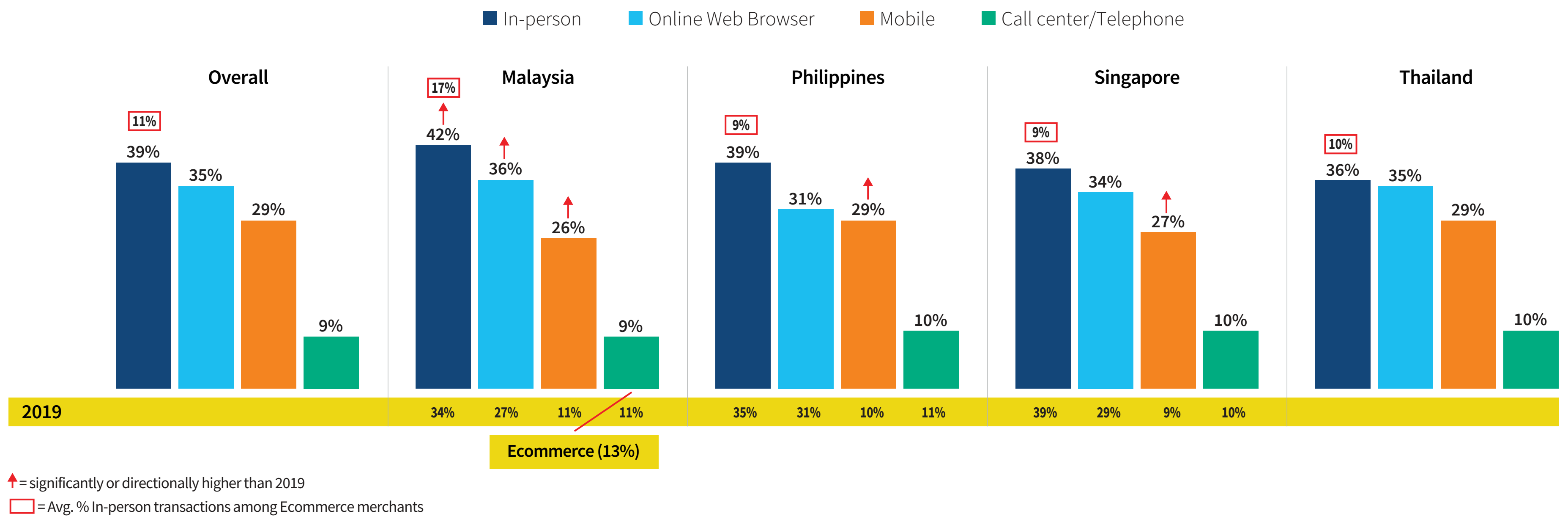
TRANSACTIONAL TRENDS

Not surprisingly, a significant majority of transactions have taken place via remote channels since the pandemic, with mobile channel volume up significantly in markets that trend from 3 years ago.

There remains a sizeable portion of online and in-person transaction volume. Online transaction volume has particularly increased in Malaysia, though a recent consumer survey has also found increased online traffic in Singapore and the Philippines as well – particularly during the COVID-19 resurgence.[7]

In-person/in-store transaction volume can include Buy Online/Pick Up in Store for both brick and mortar retailers as well as ecommerce merchants that have increasingly embraced an omnichannel approach through either opening their own physical locations or partnering with retailers for pick up.[8] Malaysian ecommerce merchants indicate nearly 20% of transaction volume involving an in-person environment.

Average Distribution of Transaction Volume Across All Channels



Survey Questions:
Q2: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following channels used by your company.

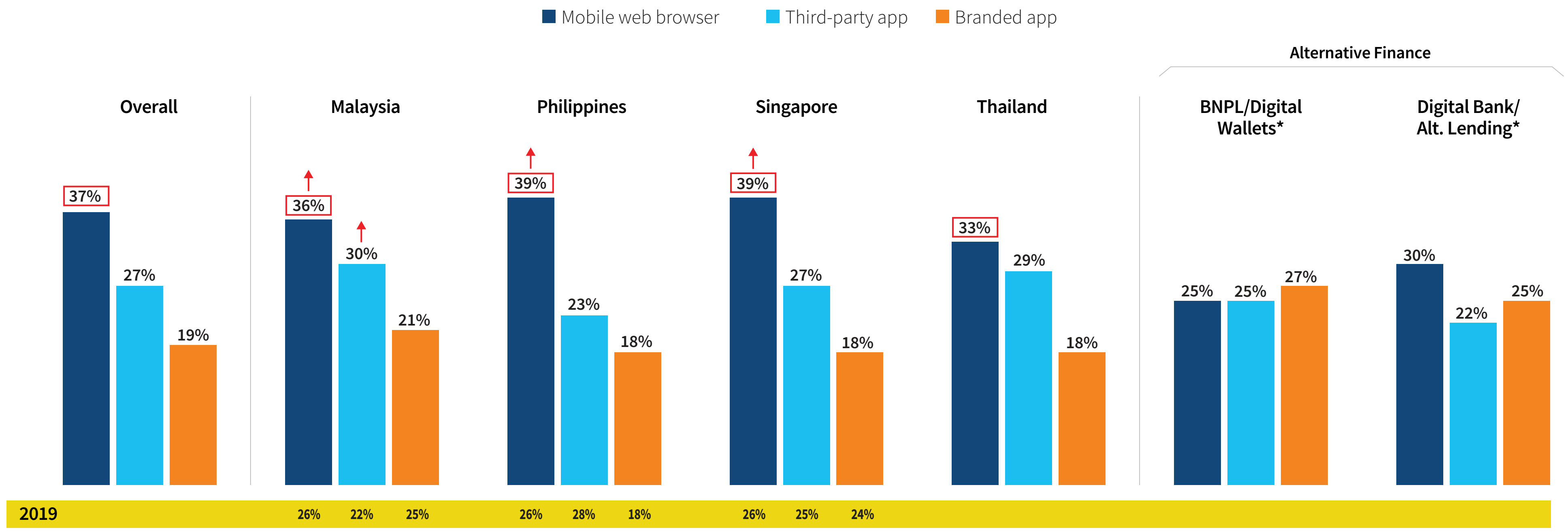
7 Https://www.cnbc.com/2021/09/16/southeast-asia-added-70-million-online-shoppers-since-covid-report.html
8 https://www.lsretail.com/resources/what-retailers-in-asia-pacific-can-teach-us-about-the-future-of-retail

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

KEY FINDING 02
TRANSACTIONAL TRENDS

Mobile transaction volume is up across mobile channels (browsers and apps).

Mobile Channel Transaction Method Use



↑ = significantly or directionally higher than 2019
☐ = significantly or directionally higher than most or all other response categories within segment/country

Survey Questions:
Q4: Please indicate the % of transactions completed (over the past 12 months) for each of the payment channels currently accepted by your company.

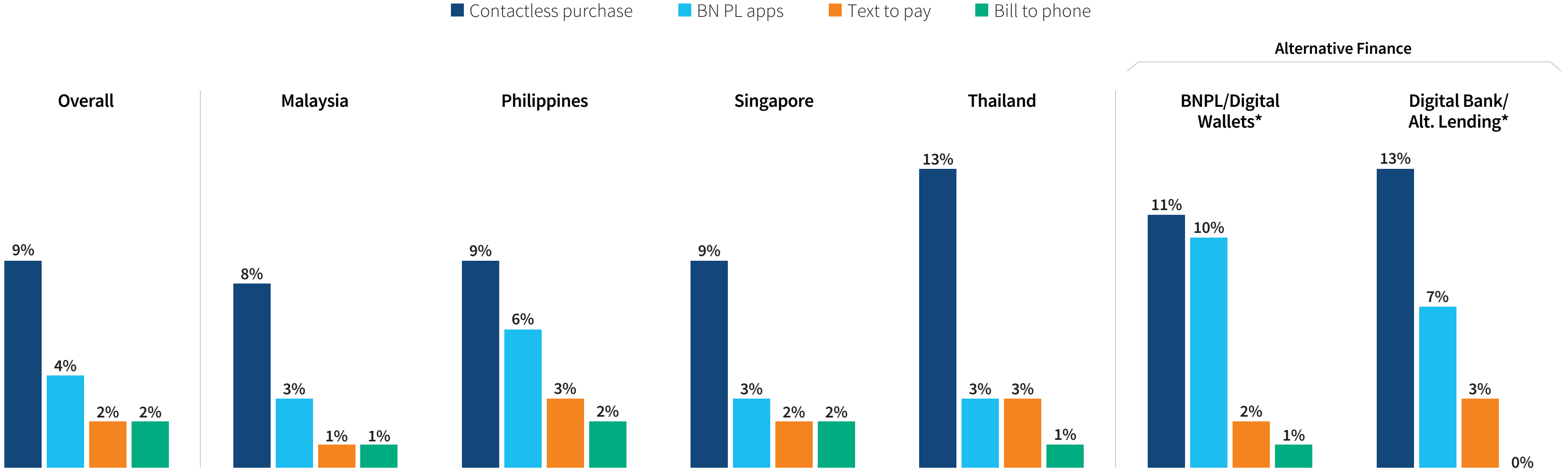
*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 02
TRANSACTIONAL TREND

Contactless payments account for roughly one-tenth of mobile channel transactions.

Mobile Channel Payment Method Use



Survey Questions:
Q4: Please indicate the % of transactions completed (over the past 12 months) for each of the payment channels currently accepted by your company.

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 03

KEY FINDING 03

The digital transformation is presenting opportunities for fraudsters, contributing to the increase in fraud costs.

The use of mobile apps and digital wallets, along with contactless payments, align with increased fraud costs. Buy Now, Pay Later (BNPL) apps account for just over one-tenth of payment method losses, which is disproportionately higher than the average volume of transactions through these apps.

Malicious bot attacks have increased during the past 12 months as the mobility of both the consumers and fraudsters have been restricted during the pandemic. In addition, a significant number of merchants and financial institutions in Asia Pacific say that fraud attacks on mobile channels have increased by up to 10% over last year.

While the point of sale has been the focus of fraud prevention efforts, new account openings and logins also account for a sizeable portion of fraud costs.

KEY FINDING 03

FRAUD TRENDS

Fraud is becoming more sophisticated and complex.

Traditional verification checkpoints, using physical attributes (physical address, date of birth, social security number, etc…), are less effective at detecting and preventing these types of organized fraud. This is particularly challenging for transactions conducted online or through mcommerce.

Sophisticated methods shown below not only impact identity risk assessment, but also transactional risk. One of these impacts is the limited ability to determine the transaction source/location.

SOPHISTICATED FRAUD

IDENTITY FRAUD RINGS

Globally organized and connected fraud networks sharing stolen identity information and collaborating with various fraud attacks. **Example use cases:** conducting bot attacks across borders; leveraging challenges posed by third-party payment providers/ gateways; use of multiple devices to confuse the trail of fraud.

SYNTHETIC IDENTITIES

Created identities comprised of real and/or fake personal information; real + fake combination makes identity seem legitimate and harder to detect using traditional, physical attribute based verification methods. **Example use cases:** nurture to establish good credit standing, ability to pass traditional verification checkpoints and then breakout to commit fraud with higher value items.

MULTIPLE DEVICE LINKAGES

Fraudulent device linked to multiple other devices via a unique shopping address. **Example use case:** purchase via mobile and pick up at store.

Several devices associated with multiple email addresses and locations. **Example use case:** create new fraudulent accounts, takeover of accounts and loyalty programs using proxy IP addresses.

BOT ATTACKS

Mobile botnet attacks. **Example use case:** malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases.

Use of stolen identities and credentials. **Example use case:** test stolen credit card information with lower value goods/services (typical of digital goods/ services) tend to arouse less suspicion; ongoing testing of identity credentials to find those which pass through retailers' identity verification checks.

Survey Questions:
Q3: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment methods currently accepted by your company.

5 https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2021/may/pandemic-alters-spending-habits-in-apac-drives-rapid-shift-to-emerging-payment-technologies/
6 FIS Worldpay, The Global Payments Report 2022; https://worldpay.globalpaymentsreport.com/en

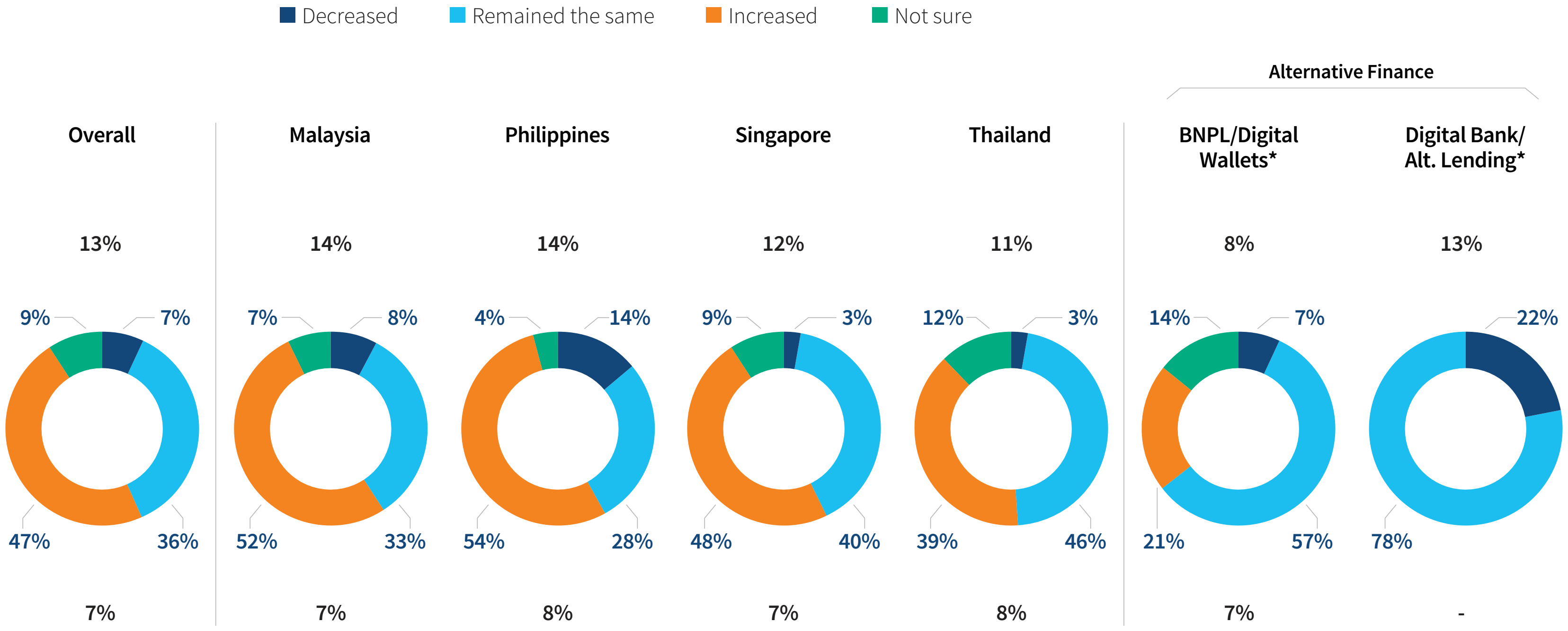
KEY FINDING 03

MALICIOUS AUTOMATED BOT ATTACKS

Malicious bot attacks have increased during the past 12 months for roughly half of merchants and financial institutions in Malaysia, Philippines and Singapore.

Across APAC, approximately 13% of transactions are determined to be malicious automated attacks.

Malicious Bot Attacks – Trends



COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

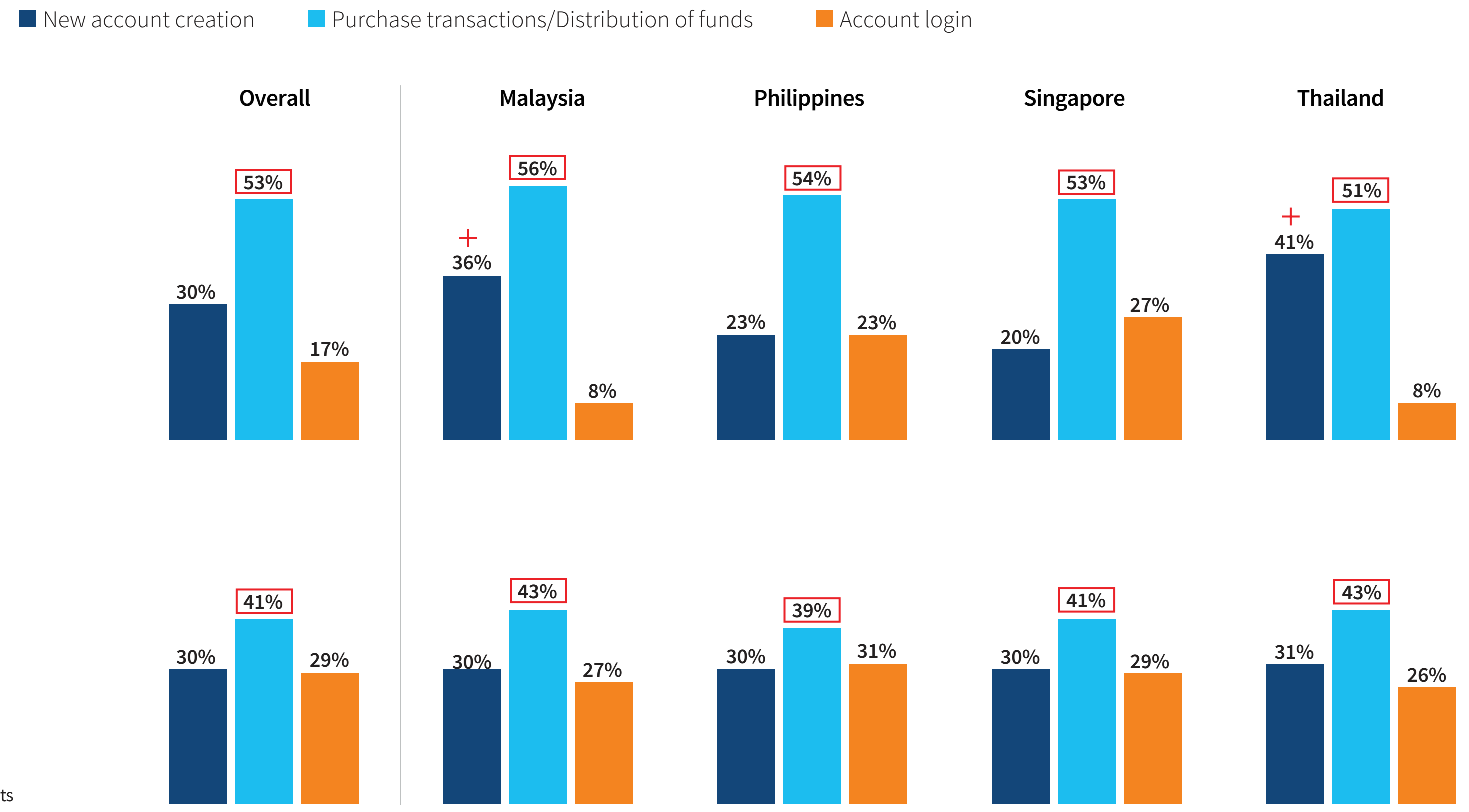
KEY FINDING 03

INCREASED LOSSES DUE TO IDENTITY AND ACCOUNT-RELATED FRAUD

APAC retailers and ecommerce merchants indicate the point of purchase as being most risky for fraud. While this journey point accounts for the larger share of fraud costs, those related to account-related fraud is still sizeable.

For some, new account creation is also a high risk point in the customer journey as well, particularly Malaysian and Thai merchants where just over one-third of losses are due to fraudulent new account creation.

Retail & Ecommerce



☐ = significantly or directionally higher than most or all other categories within market
+ = significantly or directionally higher journey stage in other markets

Survey Questions:
Q11b: Approximately, how much of your fraud losses would you attribute to each of the customer journey stages: new account creation (fraudulent new accounts), purchase transactions or distribution of funds and account login/security (i.e., related to account takeover)?
Q12n: Which of the following online customer journey stages is your organization MOST susceptible to with fraud?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 03

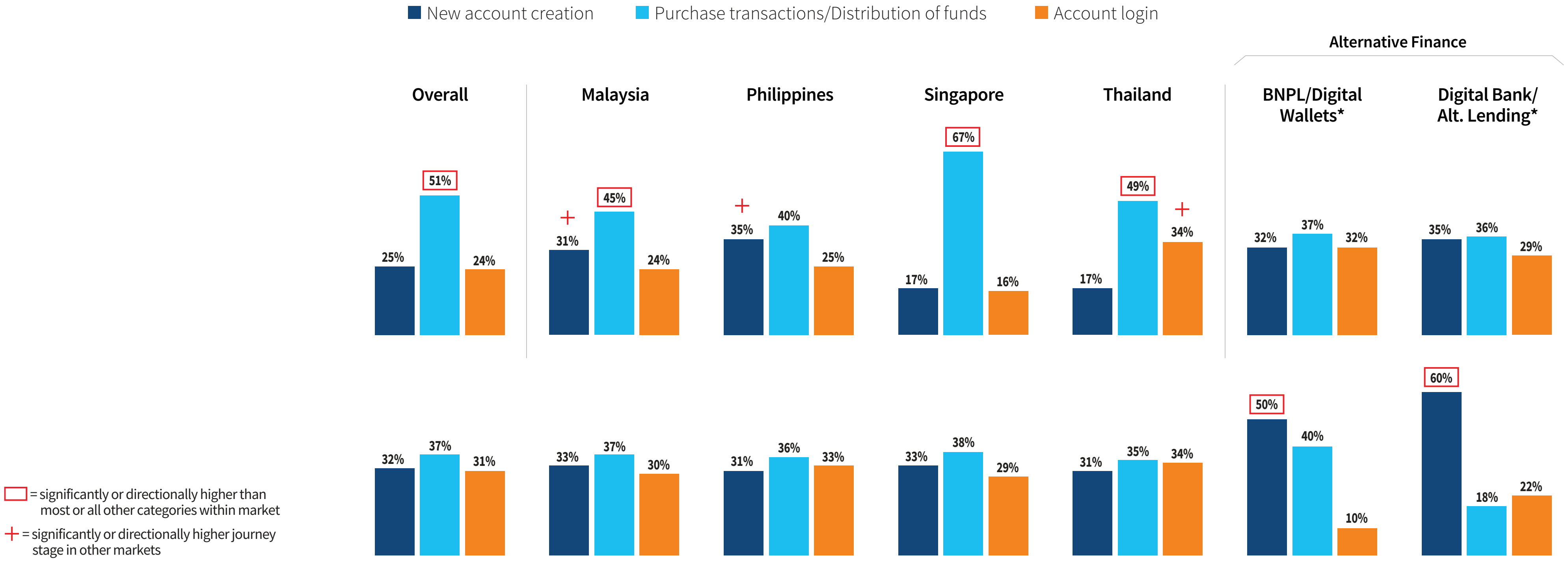
INCREASED LOSSES DUE TO IDENTITY AND ACCOUNT-RELATED FRAUD

Interestingly, distribution of funds accounts for more fraud losses, though APAC FIs attribute as much risk to account-related journey points as they do funds distribution.

A further twist is with BNPL/Digital Wallets and Digital Banking/Lending firms, which significantly view new account creation as being most risky, though their fraud losses tend to be distributed similarly across the customer journey.

BNPL/Digital Wallets providers view new account creation as being most risky; creating fraudulent accounts with BNPL providers is a tactic used by fraudsters, particularly where the application is less scrutinized and where synthetic identities make it difficult to distinguish legitimate from bogus customers.[9]

Financial Services & Lending



Survey Questions:
Q11b: Approximately, how much of your fraud losses would you attribute to each of the customer journey stages: new account creation (fraudulent new accounts), purchase transactions or distribution of funds and account login/security (i.e., related to account takeover)?
Q12n: Which of the following online customer journey stages is your organization MOST susceptible to with fraud?

9 Https://www.cnbc.com/2021/11/18/criminals-exploit-buy-now-pay-later-services-like-klarna-and-afterpay.html

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

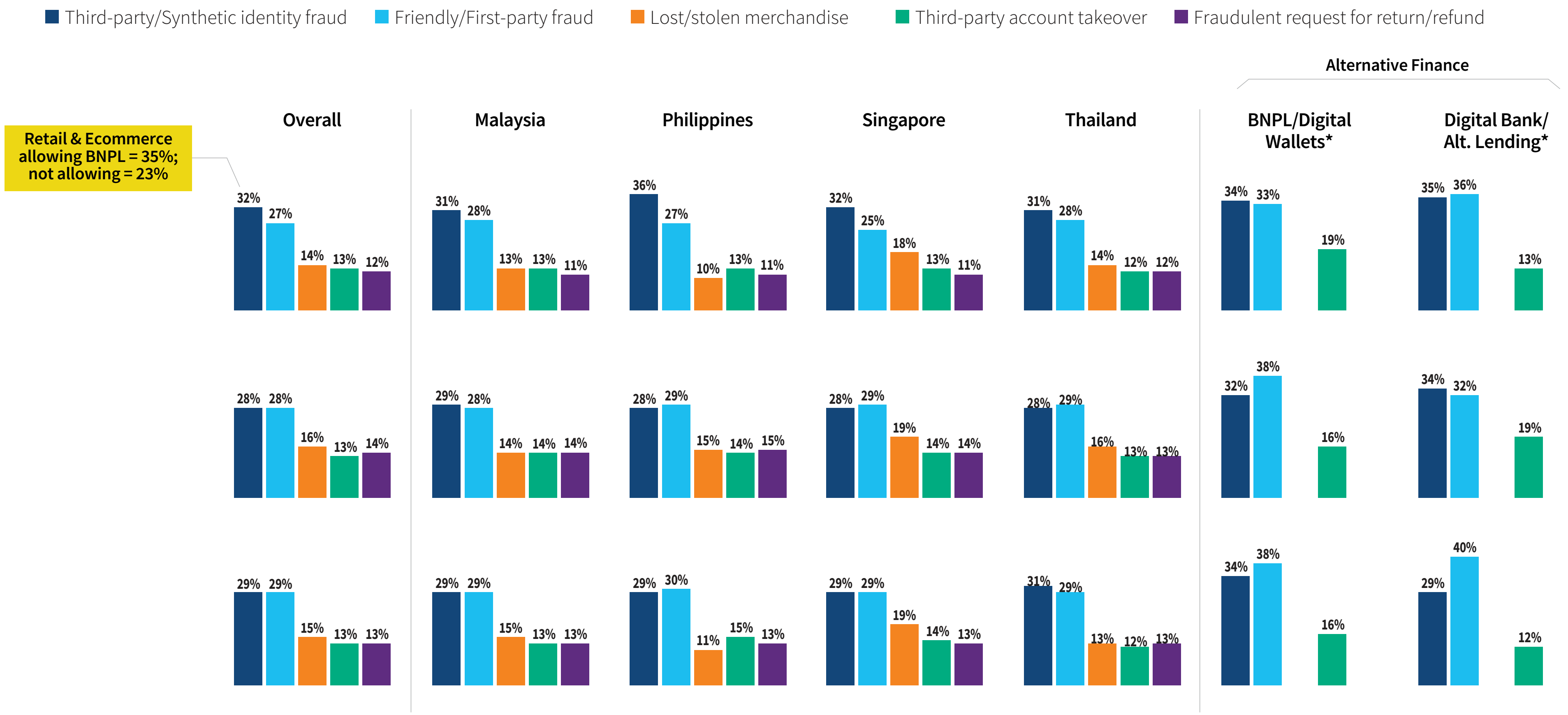
KEY FINDING 03

INCREASED LOSSES DUE TO IDENTITY AND ACCOUNT-RELATED FRAUD

Friendly/first-party and third-party/synthetic identity fraud are driving fraud losses across the customer journey.

Retail and ecommerce merchants that allow BNPL attribute a higher percentage of losses due to identity fraud at new account opening than those not allowing this payment method. This reinforces the risk that fraudsters pose at this journey stage through this emerging payment option.

% Distribution of Fraud Losses by Fraud Type



Retail & Ecommerce allowing BNPL = 35%; not allowing = 23%

Survey Questions:
Q12a: Now, continue to think about these three customer journey phases, separately and your organization's fraud losses during the past 12 months. For each specific customer journey stage, please indicate the percentage distribution your past 12-month's fraud losses across the following fraud methods.

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

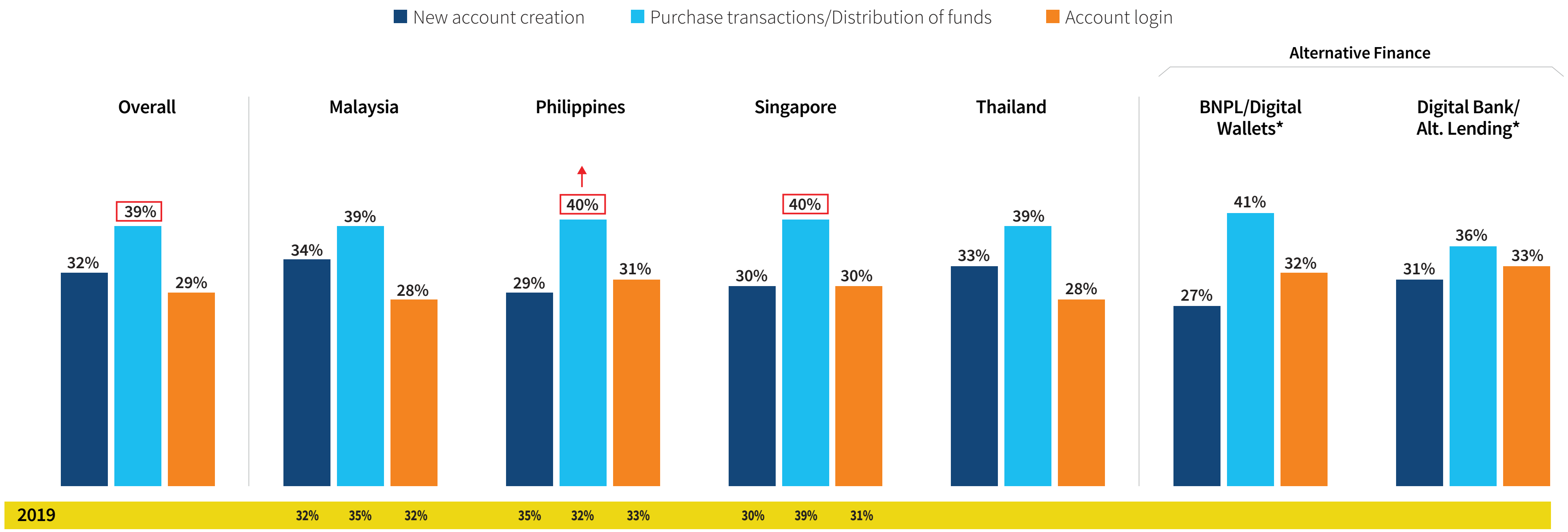
LexisNexis® RISK SOLUTIONS

KEY FINDING 03

INCREASED LOSSES DUE TO IDENTITY AND ACCOUNT-RELATED FRAUD

While point of sale directionally represents more identity-related fraud, account-related fraud is also a sizeable contribution as well.

Identity-Related Fraud: % Distribution by Activity



↑ = significantly or directionally higher than 2019
☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 03

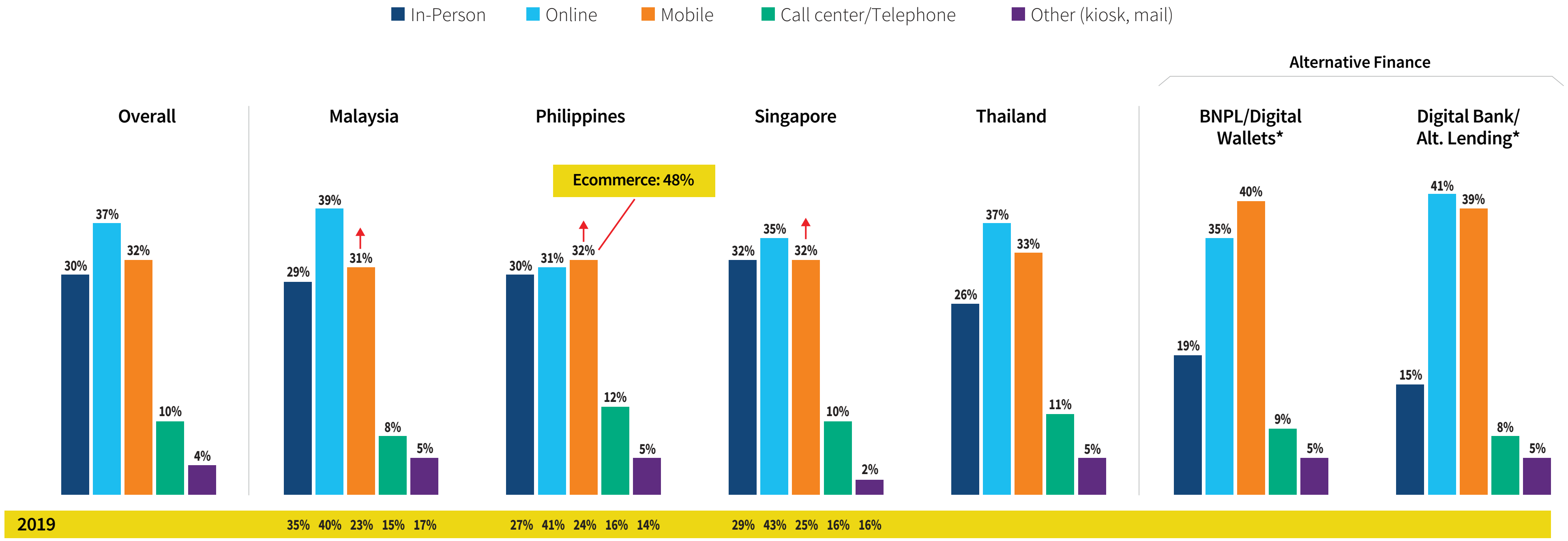
FRAUD TRENDS

The percent of fraud losses attributed to mobile channel transactions has increased since before the pandemic and is on par with online and in-person.

This follows the increase in transaction volume through the mobile channel.

Filipino ecommerce merchants attribute a significantly greater share of fraud costs to the mobile channel compared the other in other regions. This level is nearly matched by alternative finance/payment providers

% Fraud Costs by Channel*



↑ = significantly or directionally higher than 2019

Survey Questions:
Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

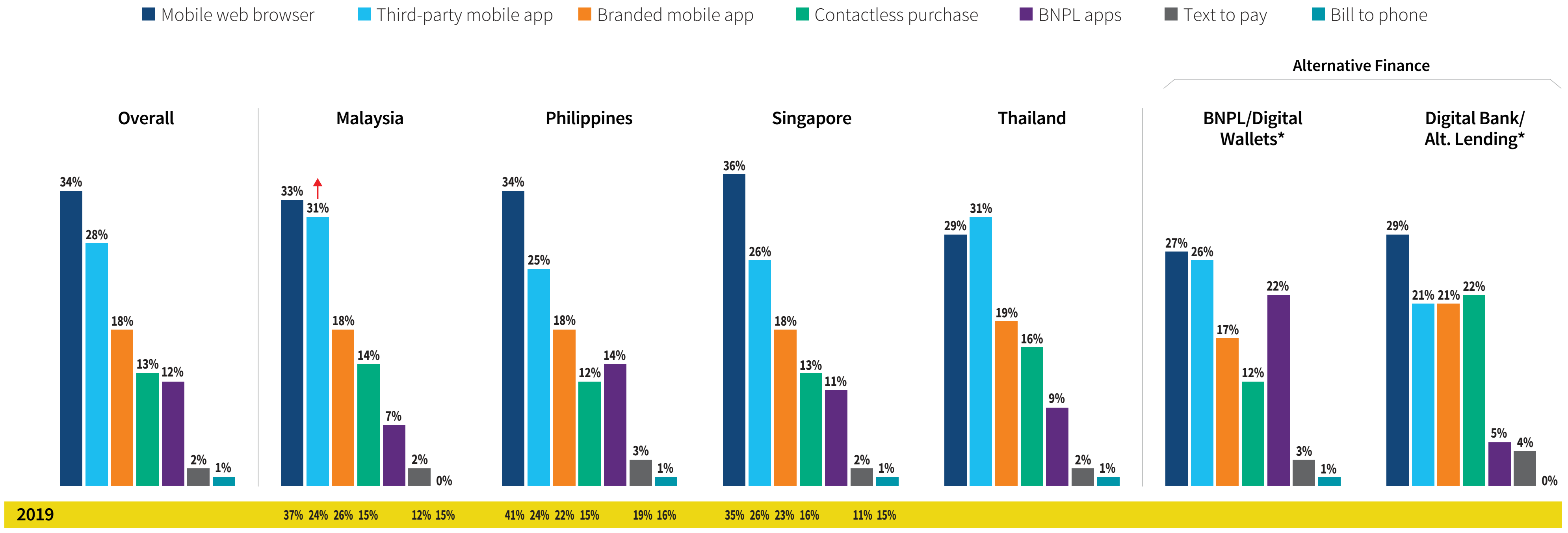
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 03
FRAUD TRENDS

While mobile browsers continue to be a sizeable portion of mobile channel fraud costs, merchants are starting to see more coming from contactless payment methods.

BNPL apps represent a similar level of fraud costs as contactless payment in the Philippines and Singapore.

Fraud Costs by Mobile Channel*



↑ = significantly or directionally higher than 2019

Survey Question:
Q17. Please indicate the distribution of fraud across the various mobile channels you use/accept

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

KEY FINDING 03

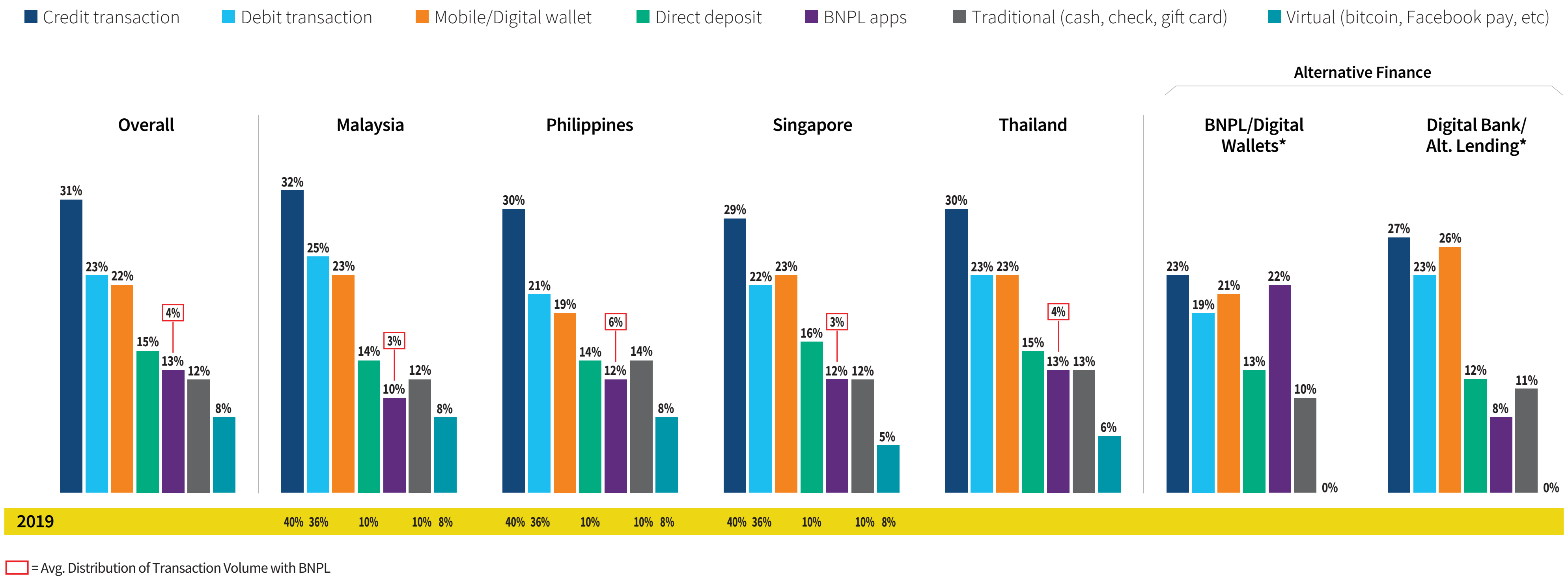
FRAUD TRENDS

While credit transactions account for the single most fraud losses by payment method, mobile and digital wallets represent a sizeable portion (nearly one-fifth).

The COVID-19 pandemic accelerated use of contactless payment methods. This payment method can pose fraud risks to merchants if breached card data is used during card enrollment process, therefore the need for strong authentication processes and tools.[10]

BNPL apps account for just over one-tenth of payment method fraud losses, though this is disproportionately higher than the average volume of transactions through this method.

% Distribution of Losses by Payment Method



Survey Question:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of fraud costs for each of the payment methods.

10 https://www.pindrop.com/blog/mobile-wallets-present-new-opportunities-for-fraud/

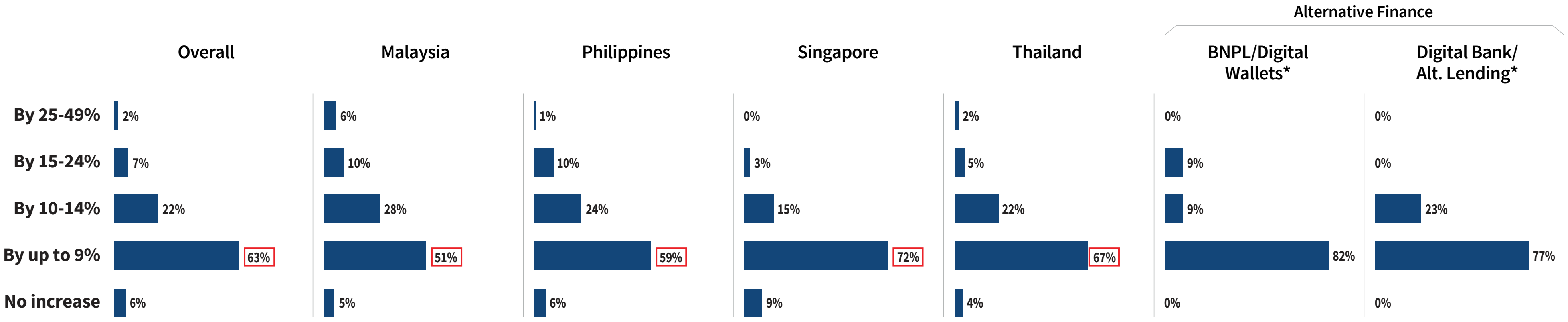
*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

KEY FINDING 03

CHANGING DISTRIBUTION OF MOBILE CHANNEL FRAUD LOSSES

As mobile transaction volume grows, fraudsters are increasingly targeting this channel, particularly alternative finance providers.

% Fraud Increase in Mobile Channel Transactions



☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q17b: To what degree has fraud that targets your mobile channel transactions increased during the past 12 months?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

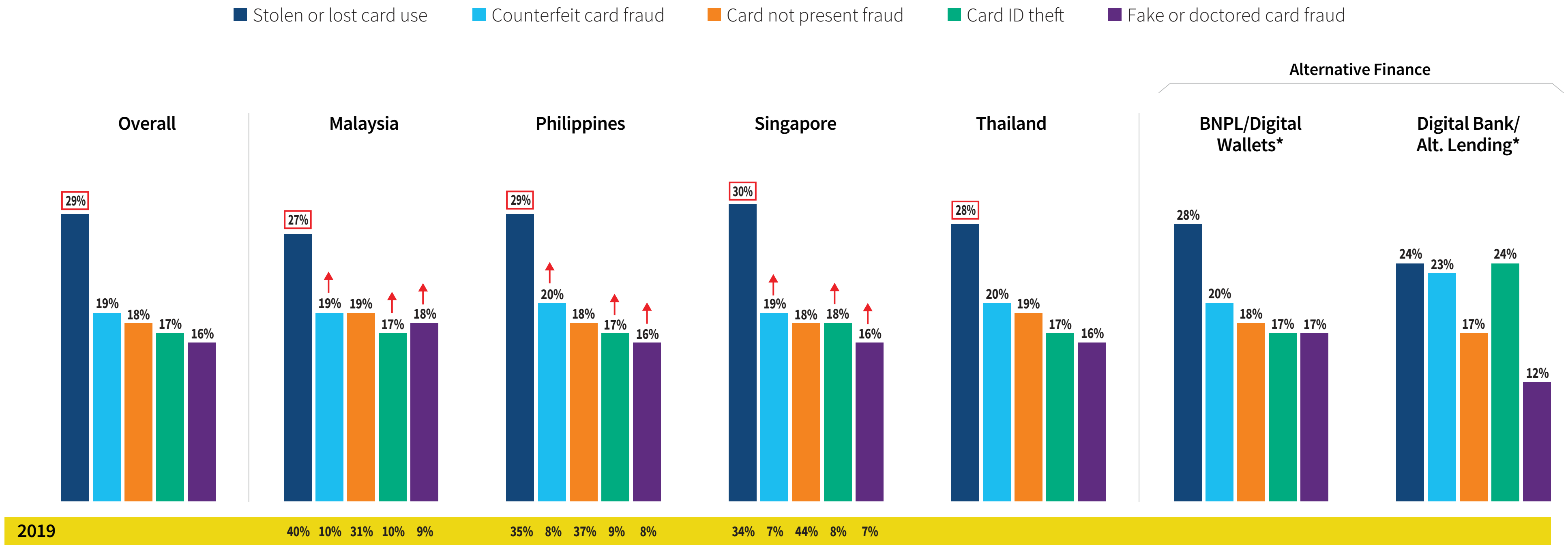
KEY FINDING 03

FRAUD TRENDS

The ways in which card-related fraud occurs is expanding beyond CNP and stolen cards to also include more counterfeit, card ID theft and use of fake/doctored cards.

BNPL is attractive for the line of credit that can be established. Fraudsters can use stolen or breached identity data to establish an account, as well as using stolen card information to repay the debt, leaving merchants with chargeback fees and BNPL providers with the loss of funds.[11]

% Distribution of Card-Related Fraud Losses



↑ = significantly or directionally higher than 2019

☐ = significantly or directionally higher than most or all other categories within market

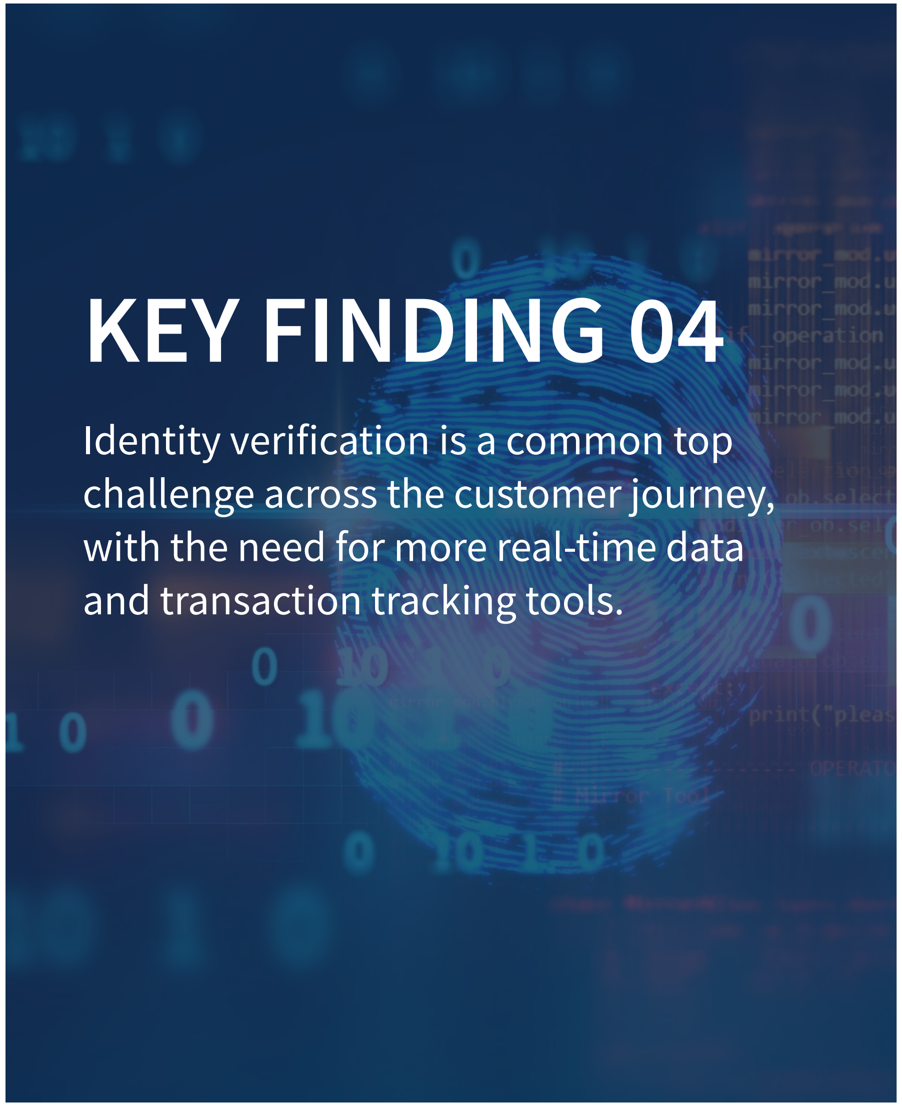
Survey Questions:
Q18e: Of your credit/debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

[11] https://www.information-age.com/fraud-scenarios-in-buy-now-pay-later-ecosystem-123497123/

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04



KEY FINDING 04

Identity verification is a common top challenge across the customer journey, with the need for more real-time data and transaction tracking tools.

Identity verification, including digital identity attributes, is particularly challenging for the account-related parts of the customer journey, such as new account opening and account login.

However, assessing the transaction risk is also a challenge, particularly at the point of sale. This includes determining the origination of the transaction and the ability to assess risks from foreign entities.

Identity theft, synthetic identities and the risk of account takeovers have accentuated the need for digital intelligence and identity authentication technology.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

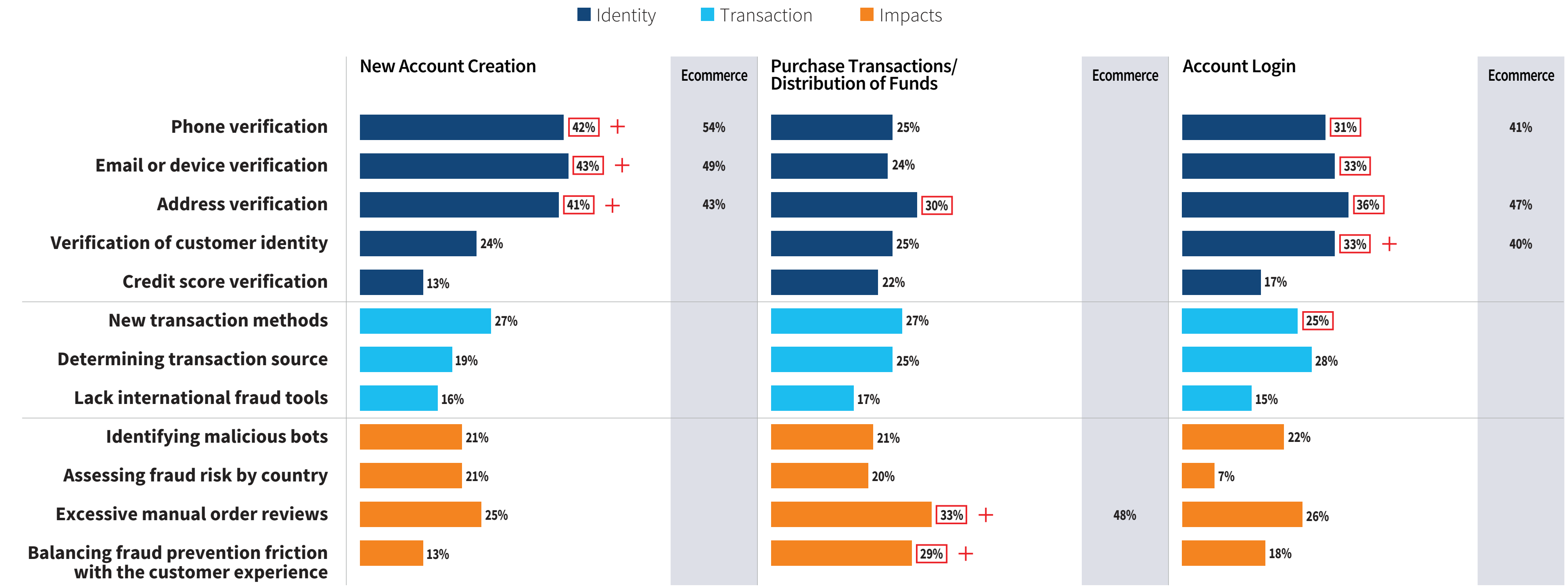
KEY FINDING 04

IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

APAC merchants and financial institutions struggle most with digital identity verification with account-related activity, particularly at the new creation stage.

Ecommerce merchants are challenged with digital identity verification significantly more than others. As shown earlier, merchants place more emphasis on point of sale as the most risky phase in the customer journey, though they are more challenged with identity verification with account-based phases – particularly at the front end of new account creation where fraudsters gain a foothold into the business. This suggests that there needs to be more focus on account-related fraud detection and mitigation.

Top Three Ranked ONLINE Fraud Challenges: Overall



☐ = significantly or directionally higher than most or all other challenges within customer journey phase
+ = significantly or directionally higher than same challenge in other customer journey phases

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online channel.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

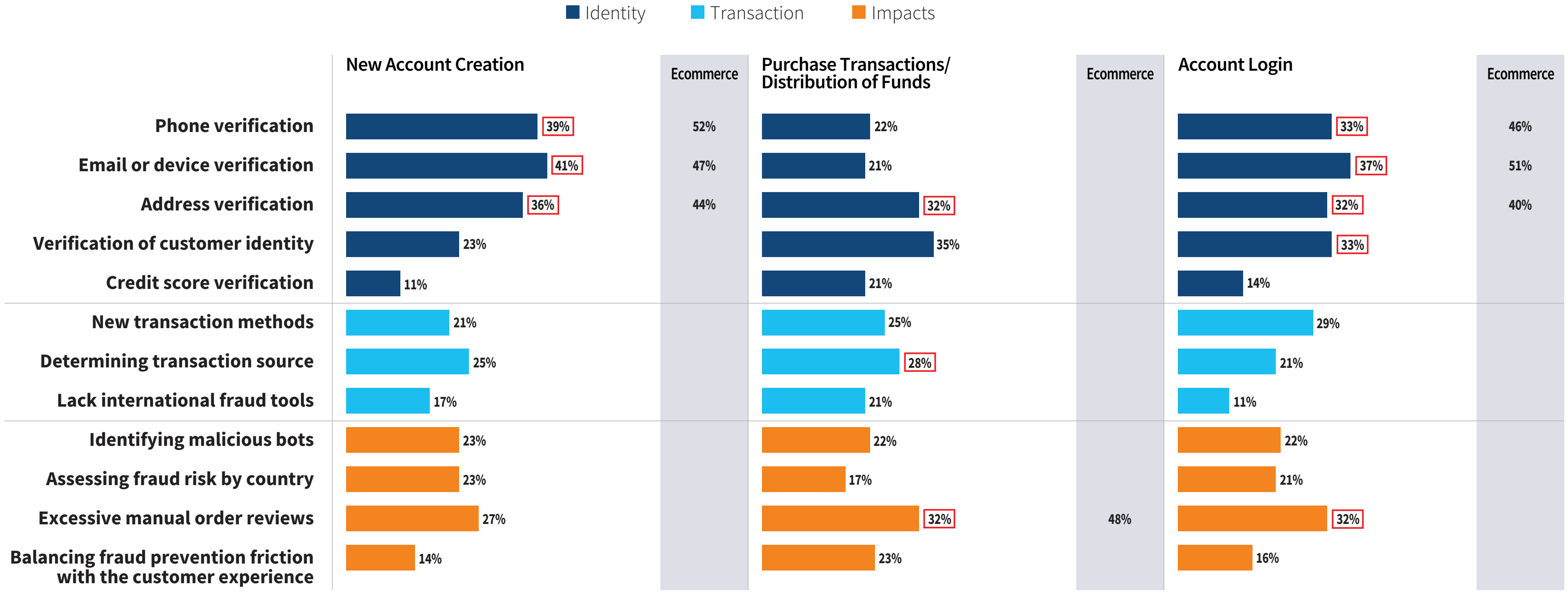
KEY FINDING 04

IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

Digital identity verification is also a mobile channel challenge for many as well, particularly with account-related activity.

As with online, ecommerce merchants are challenged with digital identity verification significantly more than others.

Top Three Ranked MOBILE Fraud Challenges: Overall



☐ = significantly or directionally higher than most or all other challenges within customer journey phase

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the mobile channel.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

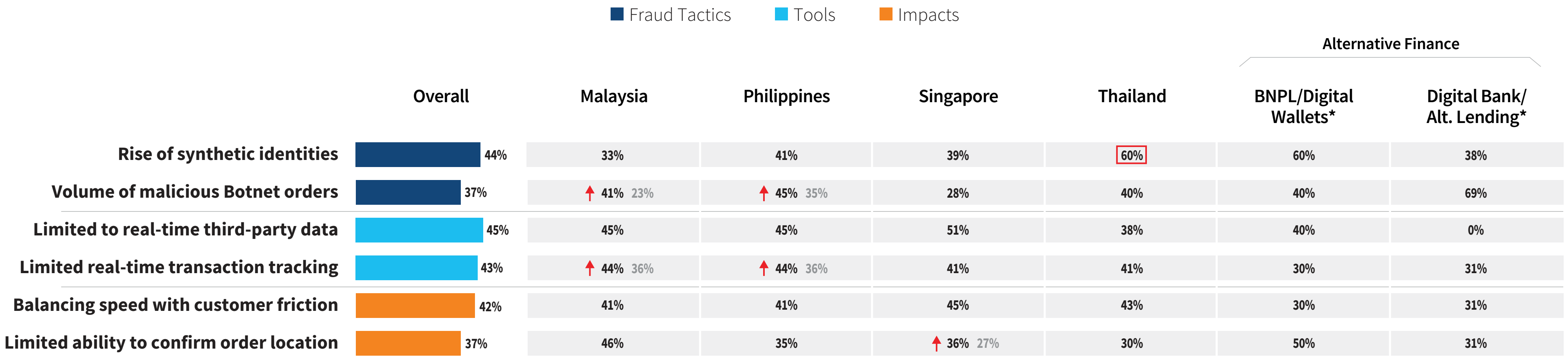
KEY FINDING 04

IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

There is need for more real-time data and transaction tracking tools to improve online channel identity verification efforts, particularly as synthetic identities and botnet volumes rise.

For countries tracking from 3 years ago, this need has grown significantly with the rise of malicious bot attacks.

Top Three Ranked Factors Making Customer Identity Verification an ONLINE CHANNEL Challenge



	Overall	Malaysia	Philippines	Singapore	Thailand	BNPL/Digital Wallets*	Digital Bank/ Alt. Lending*
Rise of synthetic identities	44%	33%	41%	39%	$\boxed{60\%}$	60%	38%
Volume of malicious Botnet orders	37%	↑ 41% 23%	↑ 45% 35%	28%	40%	40%	69%
Limited to real-time third-party data	45%	45%	45%	51%	38%	40%	0%
Limited real-time transaction tracking	43%	↑ 44% 36%	↑ 44% 36%	41%	41%	30%	31%
Balancing speed with customer friction	42%	41%	41%	45%	43%	30%	31%
Limited ability to confirm order location	37%	46%	35%	↑ 36% 27%	30%	50%	31%

↑ = significantly or directionally higher than 2019
☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q20c: Please rank the top 3 factors that make customer identity verification a challenge when serving customers through the online channel.

*Caution: small sample sizes of N=10 and N=3, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

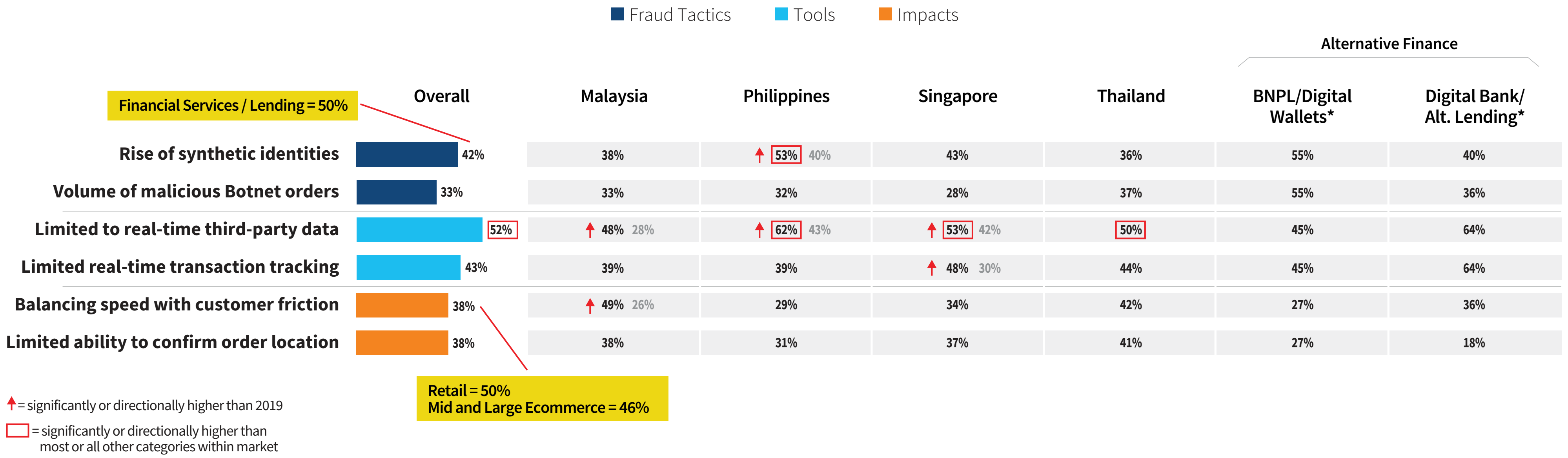
IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

There is even more need for more real-time data with mobile channel identity verification since before the COVID-19 pandemic.

For retail and ecommerce merchants, there is particular concern about balancing fraud detection and customer friction.

Financial services and lending firms, as well as BNPL and digital wallets providers, are particularly challenged by the rise of synthetic identities.

Top Three Ranked Factors Making Customer Identity Verification a MOBILE CHANNEL Challenge



	Overall	Malaysia	Philippines	Singapore	Thailand	BNPL/Digital Wallets*	Digital Bank/ Alt. Lending*
Rise of synthetic identities	42%	38%	↑ $\boxed{53\%}$ 40%	43%	36%	55%	40%
Volume of malicious Botnet orders	33%	33%	32%	28%	37%	55%	36%
Limited to real-time third-party data	$\boxed{52\%}$	↑ 48% 28%	↑ $\boxed{62\%}$ 43%	↑ $\boxed{53\%}$ 42%	$\boxed{50\%}$	45%	64%
Limited real-time transaction tracking	43%	39%	39%	↑ 48% 30%	44%	45%	64%
Balancing speed with customer friction	38%	↑ 49% 26%	29%	34%	42%	27%	36%
Limited ability to confirm order location	38%	38%	31%	37%	41%	27%	18%

↑ = significantly or directionally higher than 2019

☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q20d: Please rank the top 3 factors that make customer identity verification a challenge when serving customers through the mobile channel.

*Caution: small sample sizes of N=10 and N=3, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

MOBILE AND DIGITAL WALLETS PAYMENTS IMPACT ON FRAUD DETECTION

Given the volume and speed of mobile and digital wallets payments, these transactions can create fraud detection challenges, particularly for APAC ecommerce merchants.

Transacting through third-party payment providers also brings a level of complexity with regard to the payment chain and the end customer.

Mobile and Digital Wallets Challenges to Fraud Detection and Prevention Processes

Ecommerce = 49%	Overall	Malaysia	Philippines	Singapore	Thailand
High volume of transactions	65%	67% ☐	65% ☐	61%	66% ☐
Speed/real-time nature of value transfer	62%	66% ☐	63% ☐	51%	64% ☐
Complexity of payment chains	58%	59%	58%	50%	57%
Ensuring that payment service providers are acting in compliance with financial regulations	57%	51%	50%	58%	55%
Difficulty in determining transaction location/origination	56%	61%	57%	52%	48%
Lack of information about payment service providers' customers	56%	56%	41%	69% ☐	45%
Lack of consistency across payment applications	56%	62% +	43%	52%	56%
Volume of false positives to be reviewed	54%	57%	50%	55%	48%
% Indicating Mobile and Digital Wallets are a Challenge for Fraud Detection, Prevention	41%	40%	39%	46%	34%

☐ = significantly or directionally higher than most or all other categories within market
+ = significantly or directionally higher than all or most other markets/segments

Survey Questions:
Q20e: To what degree have mobile/digital wallets created challenges to your business's fraud detection and prevention processes/operations during the past year? Q20f: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations with transactions made through mobile/digital wallets?

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

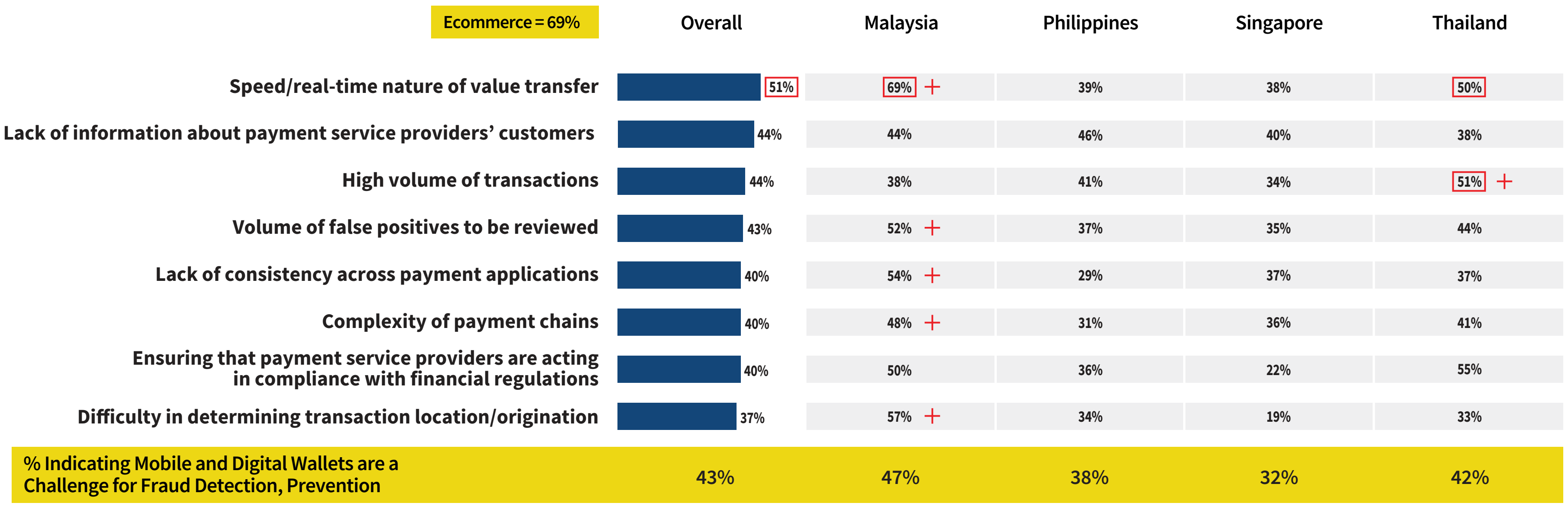
KEY FINDING 04

BNPL IMPACT ON FRAUD DETECTION

Buy Now, Pay Later apps negatively impact significantly more ecommerce merchants than do mobile and digital wallets.

Malaysian merchants particularly cite a number of challenges related to transaction speed, lack of consistency across payment applications, complexity of payment chains and determining transaction origination. This can lead to false positives and customer friction.

Buy Now, Pay Later Challenges to Fraud Detection and Prevention Processes



Ecommerce = 69%	Overall	Malaysia	Philippines	Singapore	Thailand
Speed/real-time nature of value transfer	$\boxed{51\%}$	$\boxed{69\%}$ +	39%	38%	$\boxed{50\%}$
Lack of information about payment service providers' customers	44%	44%	46%	40%	38%
High volume of transactions	44%	38%	41%	34%	$\boxed{51\%}$ +
Volume of false positives to be reviewed	43%	52% +	37%	35%	44%
Lack of consistency across payment applications	40%	54% +	29%	37%	37%
Complexity of payment chains	40%	48% +	31%	36%	41%
Ensuring that payment service providers are acting in compliance with financial regulations	40%	50%	36%	22%	55%
Difficulty in determining transaction location/origination	37%	57% +	34%	19%	33%
% Indicating Mobile and Digital Wallets are a Challenge for Fraud Detection, Prevention	43%	47%	38%	32%	42%

☐ = significantly or directionally higher than most or all other categories within market
+ = significantly or directionally higher than all or most other markets/segments

Survey Questions:
Q20e: To what degree have Buy Now, Pay Later apps created challenges to your business's fraud detection and prevention processes/operations during the past year? Q20g: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations with transactions made through Buy Now, Pay Later apps?

*Caution: small sample sizes of N=10 and N=3, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

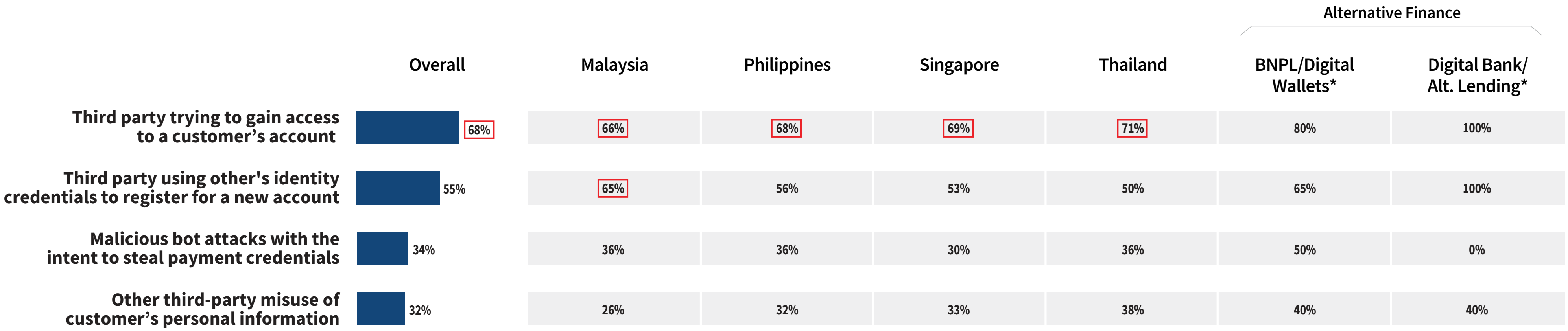
KEY FINDING 04

THIRD-PARTY FRAUD

Account-related fraud is a serious risk, with two-thirds or more APAC merchants and financial institutions saying that they've encountered third parties trying to gain access to customers' accounts during the past 12 months.

And, over half also indicate third-party use of others' credentials to establish new accounts. As mentioned earlier, fraudsters have particularly targeted Buy Now, Pay Later and digital wallets providers through the use of stolen or synthetic identities, hoping to leverage weaknesses in the application screening process.

Third-Party Misuse of Identity Credentials



	Overall	Malaysia	Philippines	Singapore	Thailand	Alternative Finance: BNPL/Digital Wallets*	Alternative Finance: Digital Bank/ Alt. Lending*
Third party trying to gain access to a customer's account	☐ 68%	☐ 66%	☐ 68%	☐ 69%	☐ 71%	80%	100%
Third party using other's identity credentials to register for a new account	55%	☐ 65%	56%	53%	50%	65%	100%
Malicious bot attacks with the intent to steal payment credentials	34%	36%	36%	30%	36%	50%	0%
Other third-party misuse of customer's personal information	32%	26%	32%	33%	38%	40%	40%

☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q20e: To what degree have Buy Now, Pay Later apps created challenges to your business's fraud detection and prevention processes/operations during the past year? Q20g: Over the past year, to what degree have the following been challenging to your fraud detection and prevention processes/operations with transactions made through Buy Now, Pay Later apps?

*Caution: small sample sizes of N=10 and N=3, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

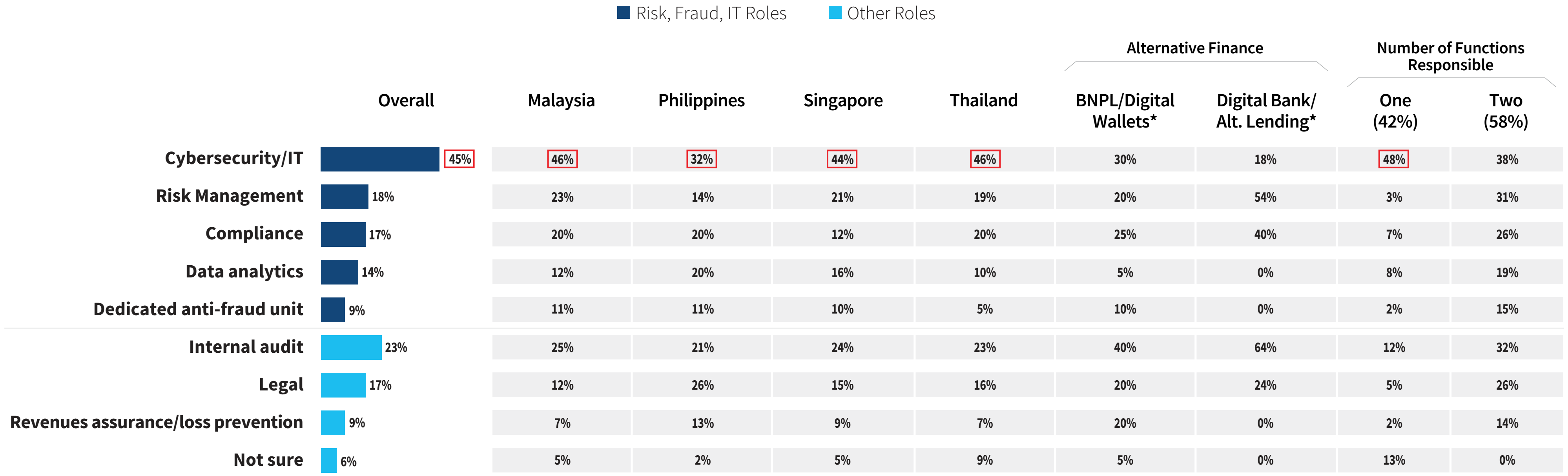
MITIGATING DIGITAL FRAUD

Whilst IT/Cybersecurity teams are often responsible for mitigating digital fraud, this responsibility can fall to other roles. It’s not necessarily clear-cut.

Most of these are within the risk, fraud or IT space, though some are not.

In many organizations, there are two functions responsible for mitigating digital fraud which vary across roles.

Departments Responsible for Mitigating Digital Fraud



						Alternative Finance		Number of Functions Responsible	
	Overall	Malaysia	Philippines	Singapore	Thailand	BNPL/Digital Wallets*	Digital Bank/ Alt. Lending*	One (42%)	Two (58%)
Cybersecurity/IT	45%	46%	32%	44%	46%	30%	18%	48%	38%
Risk Management	18%	23%	14%	21%	19%	20%	54%	3%	31%
Compliance	17%	20%	20%	12%	20%	25%	40%	7%	26%
Data analytics	14%	12%	20%	16%	10%	5%	0%	8%	19%
Dedicated anti-fraud unit	9%	11%	11%	10%	5%	10%	0%	2%	15%
Internal audit	23%	25%	21%	24%	23%	40%	64%	12%	32%
Legal	17%	12%	26%	15%	16%	20%	24%	5%	26%
Revenues assurance/loss prevention	9%	7%	13%	9%	7%	20%	0%	2%	14%
Not sure	6%	5%	2%	5%	9%	5%	0%	13%	0%

☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q31: Which department(s) is/are mainly responsible for mitigating digital fraud? Please select a maximum of two departments.

*Caution: small sample sizes of N=10 and N=3, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

KEY FINDING 05

KEY FINDING 05

Merchants and financial services firms can reduce fraud costs and risks through the best practice of adopting a multi-layered solution approach that involves the integration of cybersecurity and digital customer experience with fraud operations.

It has been a challenging exercise for businesses to find the right balance between providing security to their customers and reducing friction in the customer journey.

Digital channels have enabled businesses to reach millions of new consumers. This development has provided fraudsters new ways to launch their attacks. Moreover, these bad actors operate from across multiple locations and often use sophisticated spoofing tools to mask their true identities and locations.

The need for risk-based identity authentication to fend off fraud attacks is stronger than ever. Fraud prevention is a multi-faceted strategy that looks at the customer journey in its entirety.

On average, many businesses are not optimizing their fraud detection and prevention approaches based on this best practice. Those that embrace it are more likely to have data they need to detect and assess fraud risks and verify and authenticate both the physical and digital identity of a person with less need for manual reviews. They will thus have a lower cost of fraud.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

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 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 a 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 transaction patterns of an individual against their current transactions to detect if volume by the cardholder matches 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:** check verification services; payment instrument authentication; name/address/DOB verification.

Active ID authentication: use of personal data known to the customer for authentication; or where a 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/behavioral biometrics: analyzes human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment; browser/malware tracking; device ID/fingerprinting.

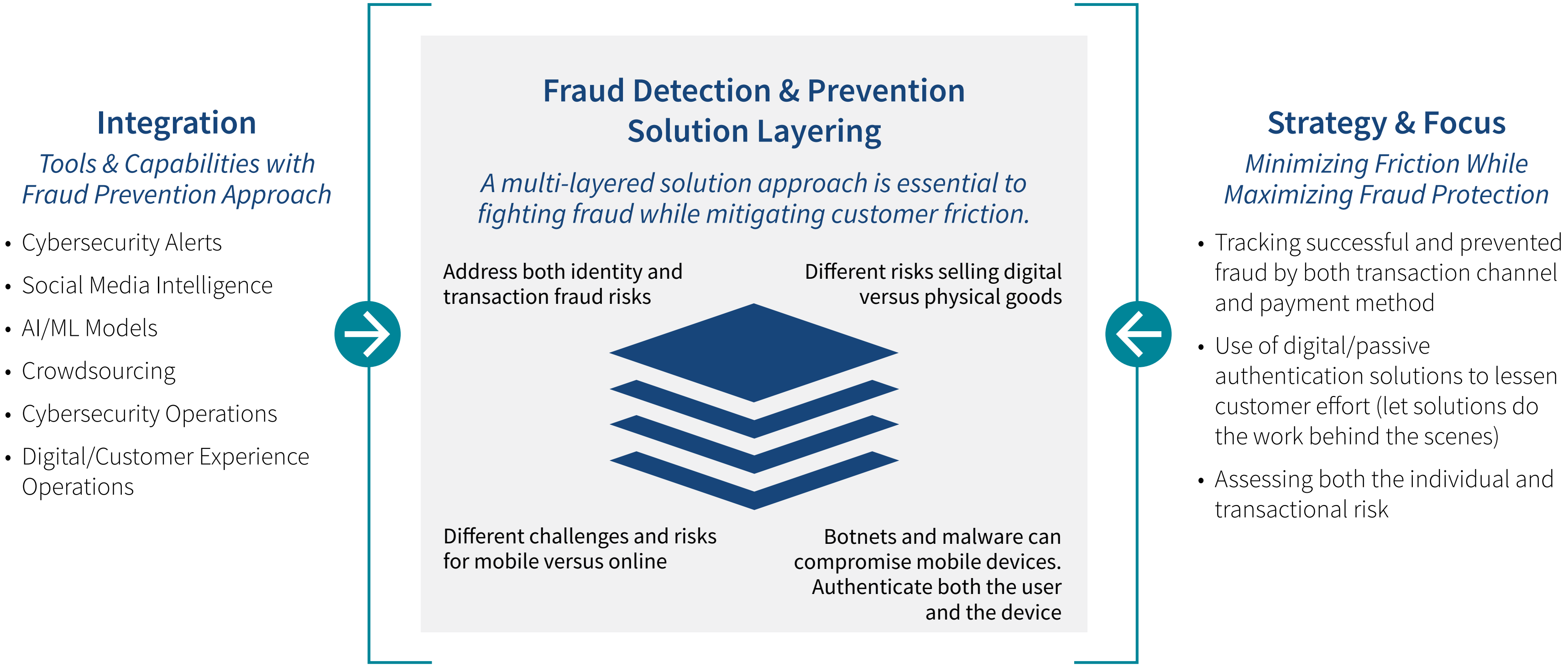
Device assessment: uniquely identify a remote computing device or user. **Solution examples:** device ID/fingerprint; geolocation.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Best practice approaches involve a layering of different solutions to address unique risks from different channels, payment methods and products. And they go farther by integrating capabilities and operations with their fraud prevention efforts.



Integration

Tools & Capabilities with Fraud Prevention Approach

- Cybersecurity Alerts
- Social Media Intelligence
- AI/ML Models
- Crowdsourcing
- Cybersecurity Operations
- Digital/Customer Experience Operations

Fraud Detection & Prevention Solution Layering

A multi-layered solution approach is essential to fighting fraud while mitigating customer friction.

Address both identity and transaction fraud risks

Different risks selling digital versus physical goods

Different challenges and risks for mobile versus online

Botnets and malware can compromise mobile devices. Authenticate both the user and the device

Strategy & Focus

Minimizing Friction While Maximizing Fraud Protection

- Tracking successful and prevented fraud by both transaction channel and payment method
- Use of digital/passive authentication solutions to lessen customer effort (let solutions do the work behind the scenes)
- Assessing both the individual and transactional risk

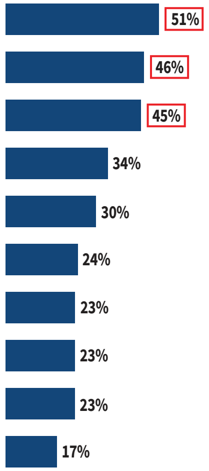
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD METRICS

Metrics used for measuring fraud performance vary widely in APAC, with manual review, order approval and average order time rates used by around half of organizations.

Measuring Fraud Prevention Performance



						Alternative Finance	
	Overall	Malaysia	Philippines	Singapore	Thailand	BNPL/Digital Wallets*	Digital Bank/ Alt. Lending*
Manual review rates	$\boxed{51\%}$	$\boxed{46\%}$	$\boxed{60\%}$	$\boxed{56\%}$	36%	60%	24%
Order approval rates	$\boxed{46\%}$	$\boxed{41\%}$	46%	45%	$\boxed{48\%}$	45%	40%
Average time for order reviews	$\boxed{45\%}$	$\boxed{44\%}$	$\boxed{51\%}$	37%	$\boxed{50\%}$	65%	54%
Total decline rates	34%	28%	31%	43%	32%	35%	18%
Abandonment rates	30%	31%	39%	31%	26%	30%	76%
False positive rates	24%	22%	34%	22%	24%	35%	22%
Early payment default rates	23%	17%	25%	19%	31%	20%	18%
Chargeback rates	23%	27%	17%	24%	24%	45%	42%
Automatic decline ratio	23%	33%	26%	13%	30%	20%	24%
Fraud loss costs to sale ratio	17%	19%	15%	13%	21%	20%	40%

$\boxed{}$ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q12c: Which of the following metrics does your organization use to measure its performance with preventing fraud

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

LexisNexis® RISK SOLUTIONS

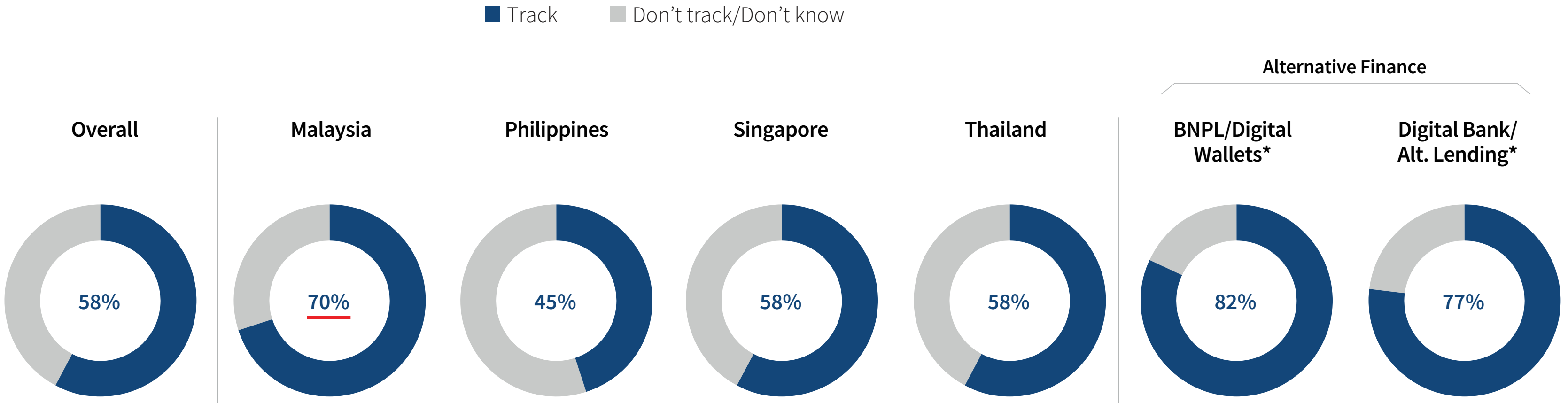
KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

APAC financial institutions are more likely to track fraud costs by point of origination, though that varies by market.

Malaysian financial services, lending, retail and ecommerce merchants are more advanced with this best practice than other markets. This is followed by at least financial services and lending firms in Singapore. Alternative finance providers are also very likely to track point of origin.

% Track The Cost of Fraudulent Transactions by Where They Originate Internationally



	Overall	Malaysia	Philippines	Singapore	Thailand
Financial Services & Lending	70%	78%	55%	81%	65%
Retail & Ecommerce	58%	70%	48%	55%	59%

— = significantly or directionally higher than same solution in the other customer journey phase

Survey Questions:
Q14b: Does your company track the cost of fraudulent transactions by where they originate internationally (i.e., coming from specific regions)?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

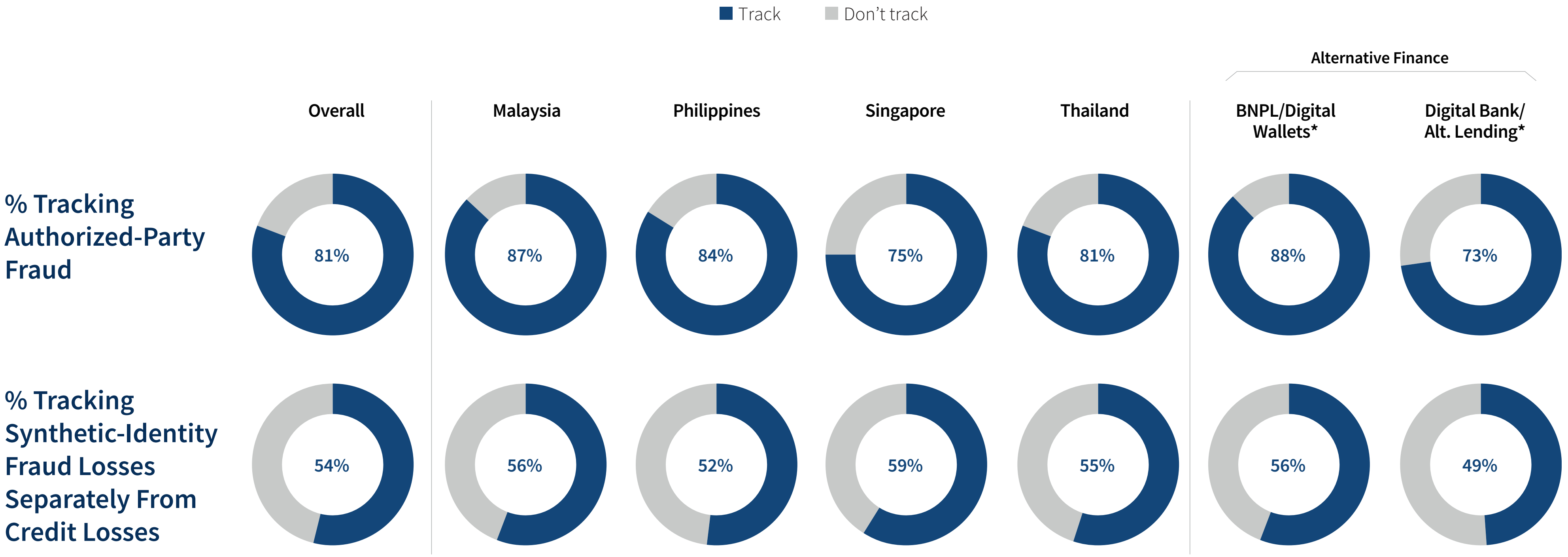
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

A significant majority of APAC merchants and financial institutions that they track authorized-party fraud.

Fewer, however, report tracking synthetic-identity fraud losses separately from credit losses.



Survey Questions:
Q14c: Does your organization track authorized-party fraud in its overall measurement of payment method fraud?
Q14d: Does your organization track synthetic-identity fraud losses separately from credit losses?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

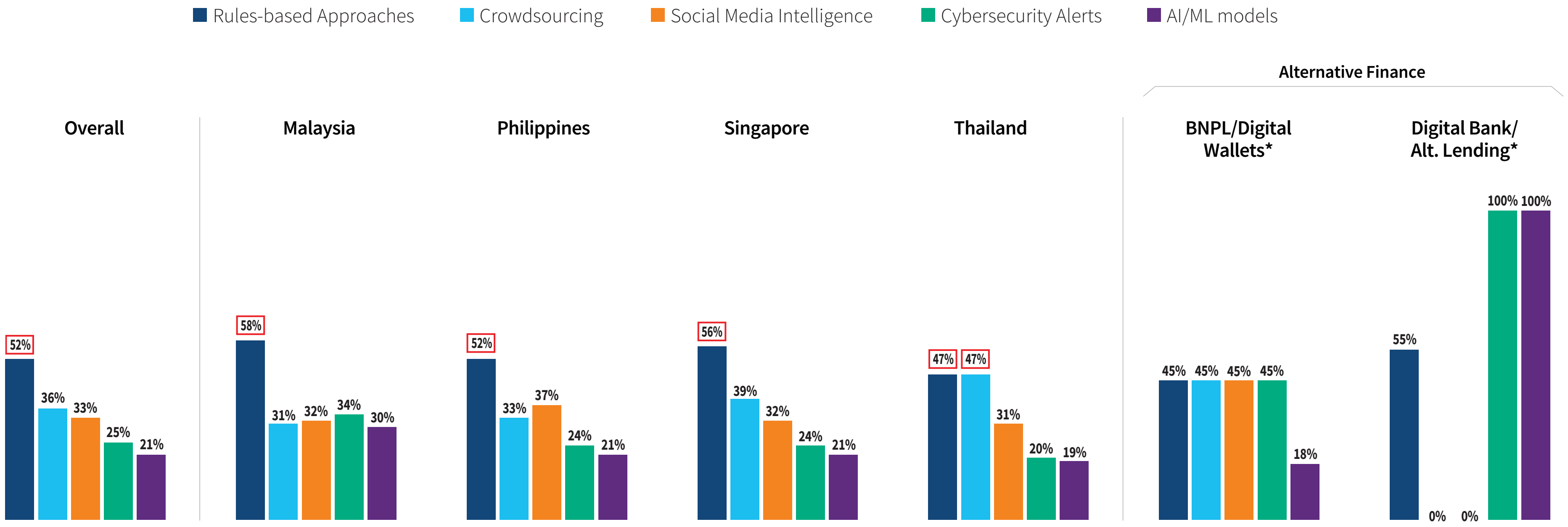
KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Few indicate using different types of supportive capabilities to fight fraud, other than half reporting use of rules-based approaches.

AI/ML models and Social Media intelligence, which are not widely used for fraud detection, can support digital identity verification and transactional risk through behavioral analytics. Cybersecurity alerts can protect against bot attacks. Limited use of these supportive capabilities can weaken fraud detection and mitigation efforts during the rise of the digital transformation.

% Using Supportive Capabilities to Fight Fraud



☐ = significantly or directionally higher than most or all other categories within market

Survey Questions:
Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?
*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

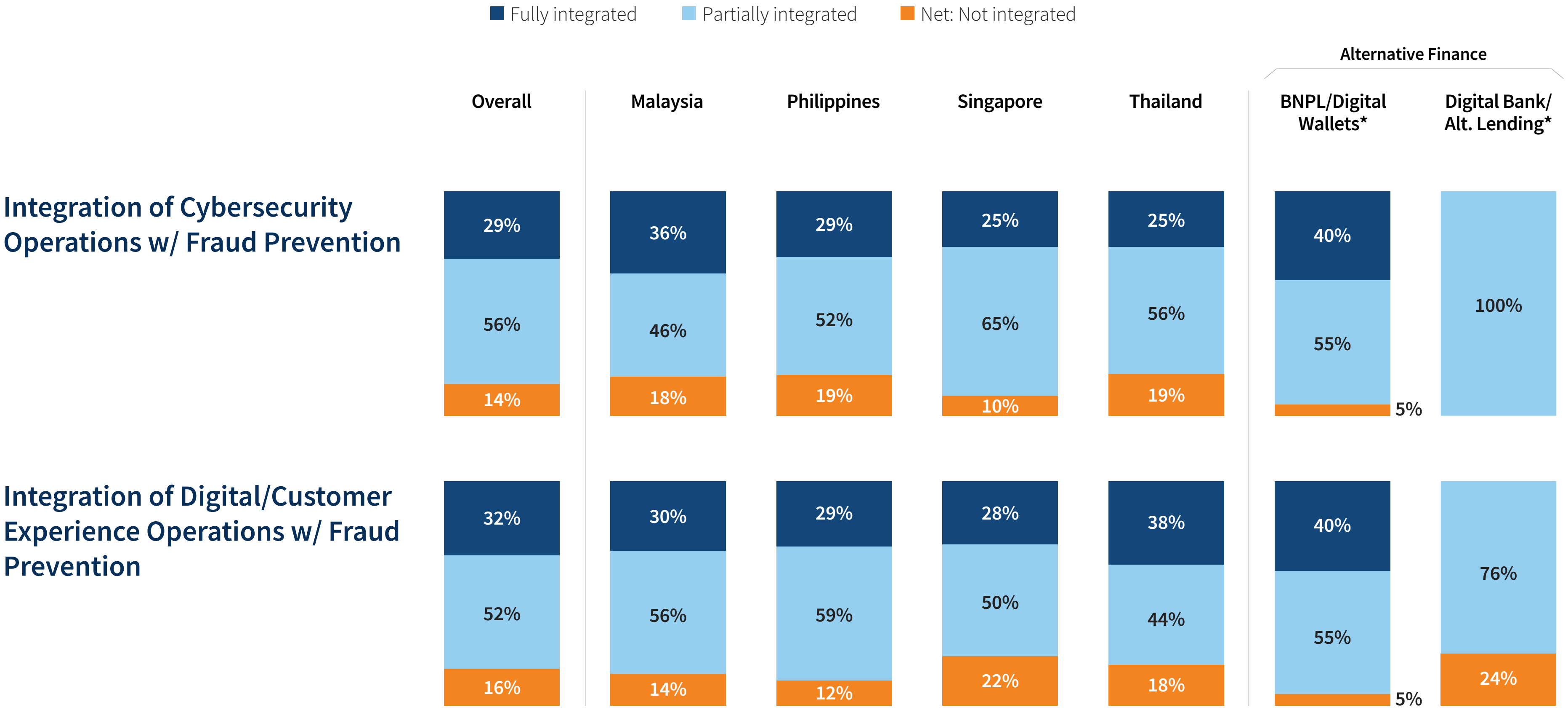
Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Few have fully integrated their cybersecurity and digital/customer experience operations with fraud prevention, though most are working towards this.

This type of integration protects against fraud attacks in this digital age, and lessens the potential for customer friction. Where customers become victims to account takeover, organizations lose more than just the fraud value and cost; there is also the loss of customer trust and brand reputation that can put future revenue streams at risk.



Survey Questions:
Q29: To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts?
*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

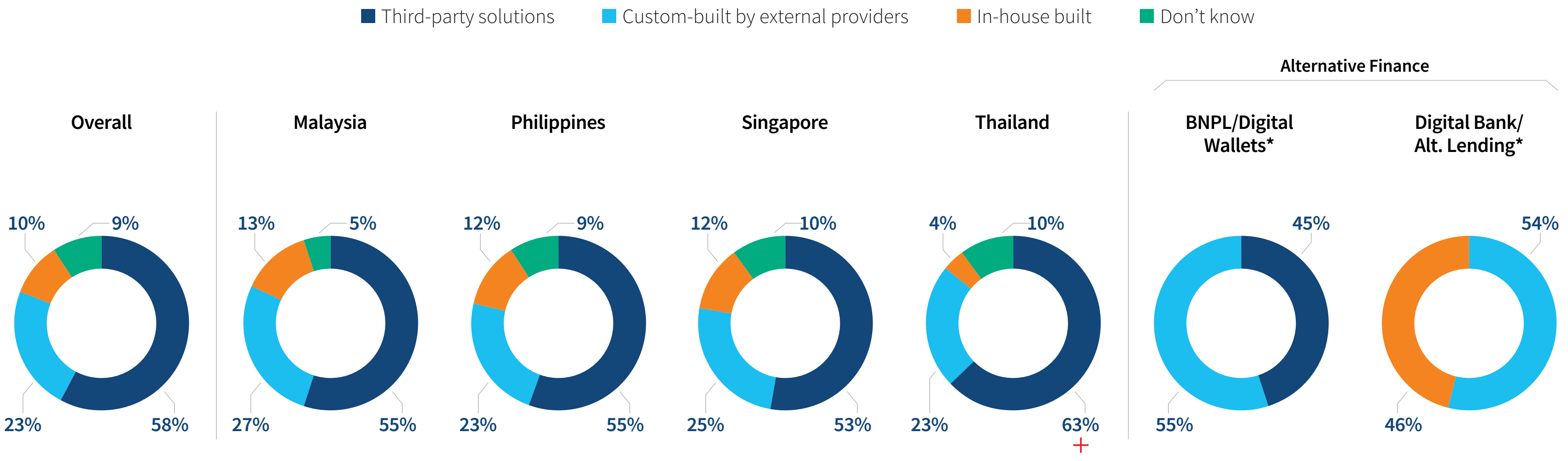
KEY FINDING 05

COMBATTING DIGITAL FRAUD

Third-party providers are heavily relied on for combatting digital fraud, either through implementation of their own solutions or support with custom-built solutions for customers.

Few organizations are building their own in-house solutions to combat this type of fraud, which indicates recognition of it's complexity and the need for expert resources and guidance. The exception to this might be among digital banks/alternative lenders.

Technology Used to Combat Digital Fraud



+ = significantly or directionally higher than all or most other markets/segments

Survey Questions:
Q32: What best describes your main current technology to combat digital fraud?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

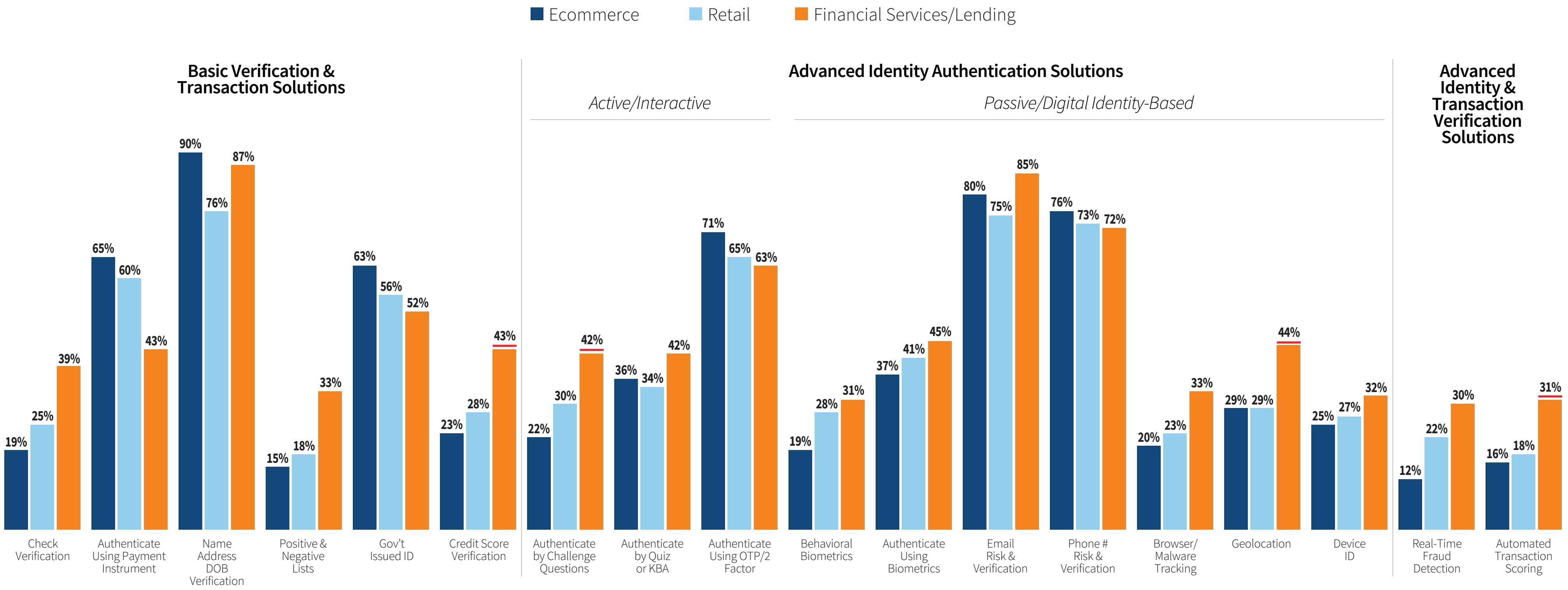
KEY FINDING 05
FRAUD DETECTION & PREVENTION APPROACHES

However, retail/ecommerce solutions approaches may not be optimal. Email/phone number risk verification and OTP/2 factor authentication use is high. But, there is limited layering of other digital solutions to assess mobile channel and transaction risk.

Digital identity solutions are designed to assess both individual and device risks (Email/Phone Risk Verification, Geolocation, Device ID, Browser/Malware Tracking) and, for some, risk of the transaction (Automated Transaction Scoring). Geolocation and Device ID also support mobile channel fraud detection. All of these mentioned solutions provide fast, seamless and "behind the scenes" fraud detection that reduces customer efforts and delays.

Fraud Mitigation Solutions Use

(APAC: Malaysia, Philippines, Thailand, Singapore)



— = significantly or directionally higher than same solution in the other customer journey phase

Survey Questions:
Q27: Which of the following fraud solutions does your company currently use?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

KEY FINDING 05

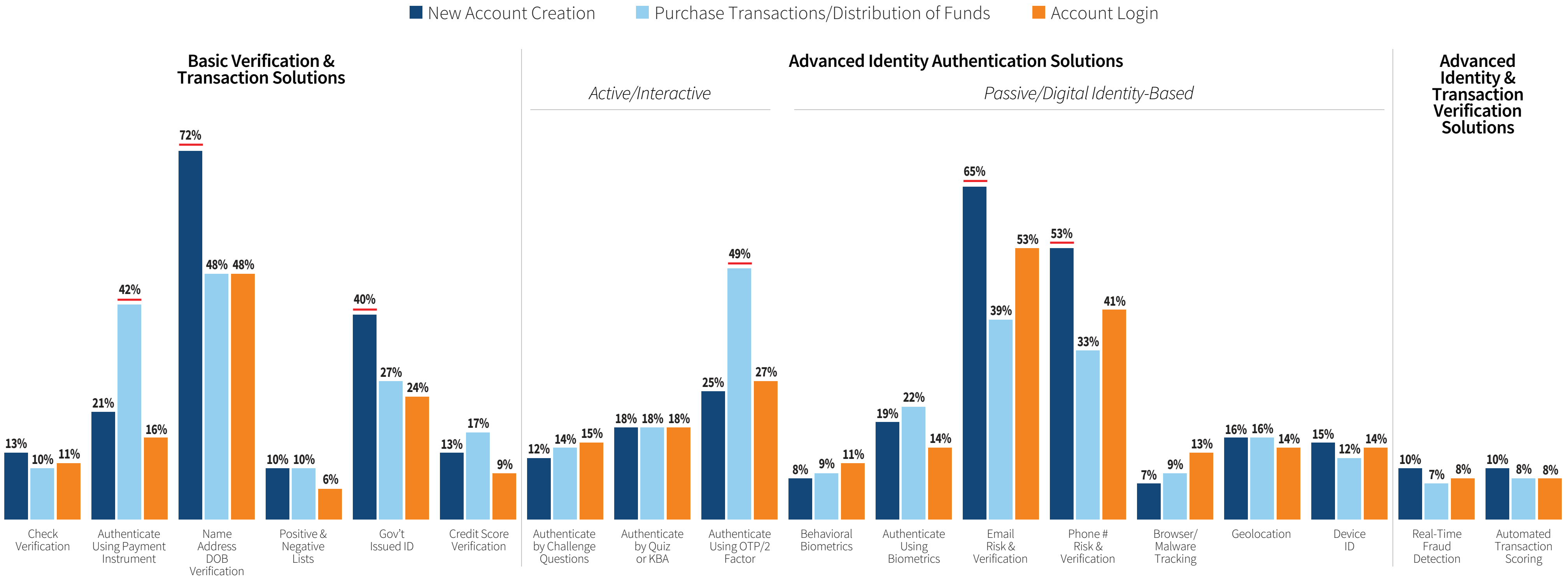
FRAUD DETECTION & PREVENTION APPROACHES

There also tends to be use of the same solutions across the customer journey phases, even though risks and challenges differ between account creation/login and purchasing.

Digital identity solutions are designed to assess both individual and device risks (Email/Phone Risk Verification, Geolocation, Device ID, Browser/Malware Tracking) and, for some, risk of the transaction (Automated Transaction Scoring). Geolocation and Device ID also support mobile channel fraud detection. All of these mentioned solutions provide fast, seamless and "behind the scenes" fraud detection that reduces customer efforts and delays.

Fraud Mitigation Solutions Use

(APAC: Malaysia, Philippines, Thailand, Singapore)



— = significantly or directionally higher than same solution in the other customer journey phase

Survey Questions:
Q27: Which of the following fraud solutions does your company currently use?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

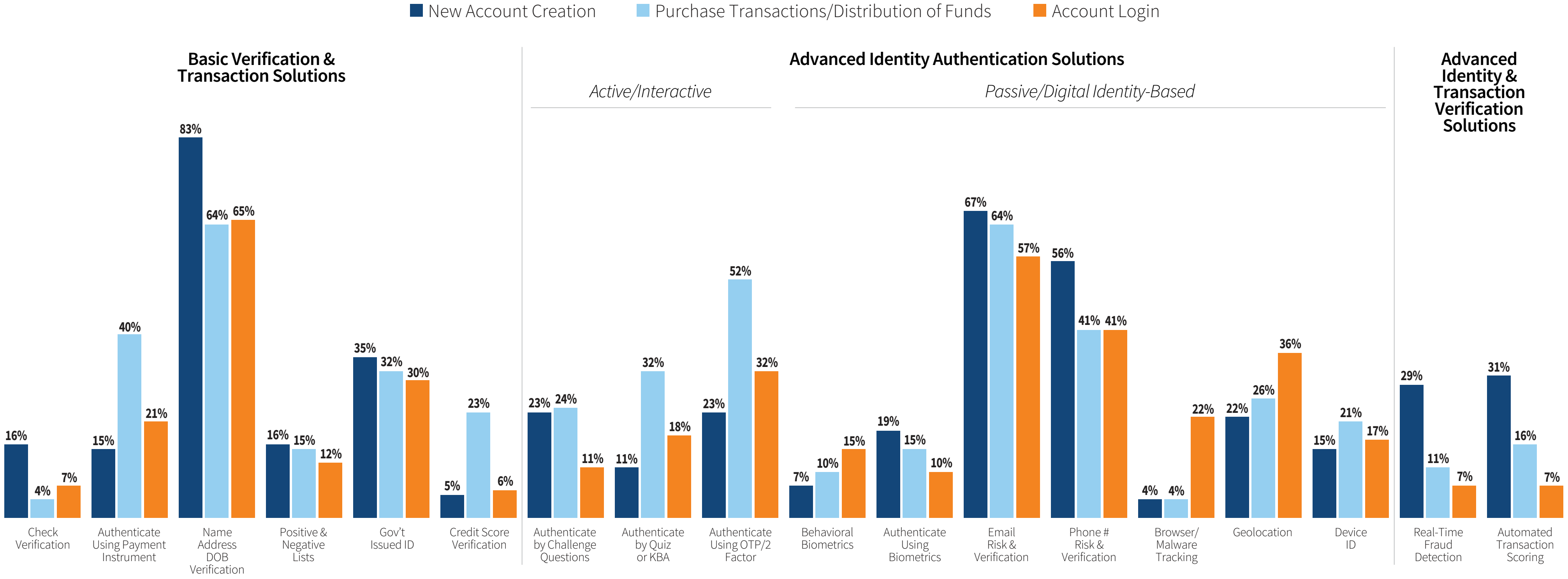
KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Alternative finance/payment providers are also not optimizing their solutions strategy.

Fraud Mitigation Solutions Use

(Alternative Finance*: BNPL, Digital Wallets, Digital Bank, Alternative Lending)



Survey Questions:
Q27: Which of the following fraud solutions does your company currently use?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

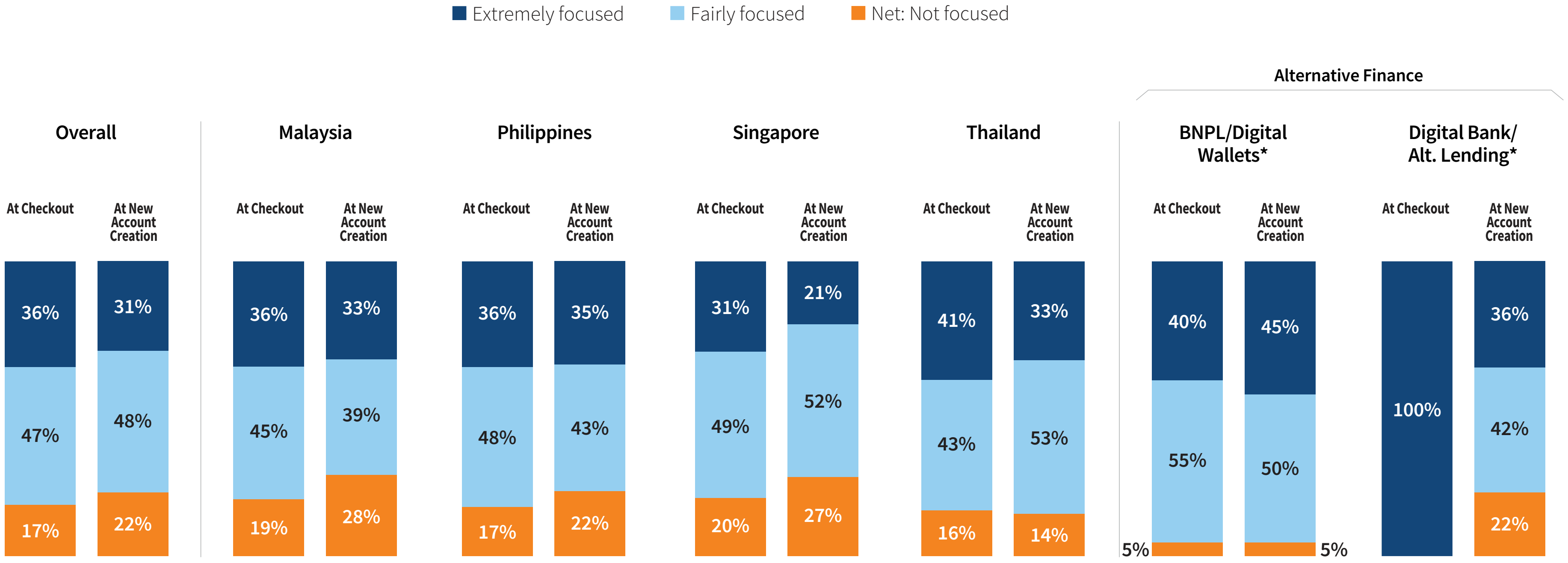
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

There is moderate focus on optimizing fraud detection with minimal customer friction among APAC merchants and financial institutions.

Degree of Focus on Optimizing Risk Level to Appropriate Customer Friction Level



Survey Questions:
Q30: To what degree is your company focused on minimizing customer friction during an online or mobile channel transaction checkout?
Q30a: To what degree is your company focused on minimizing customer friction when someone opens a new account online or through a mobile device?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

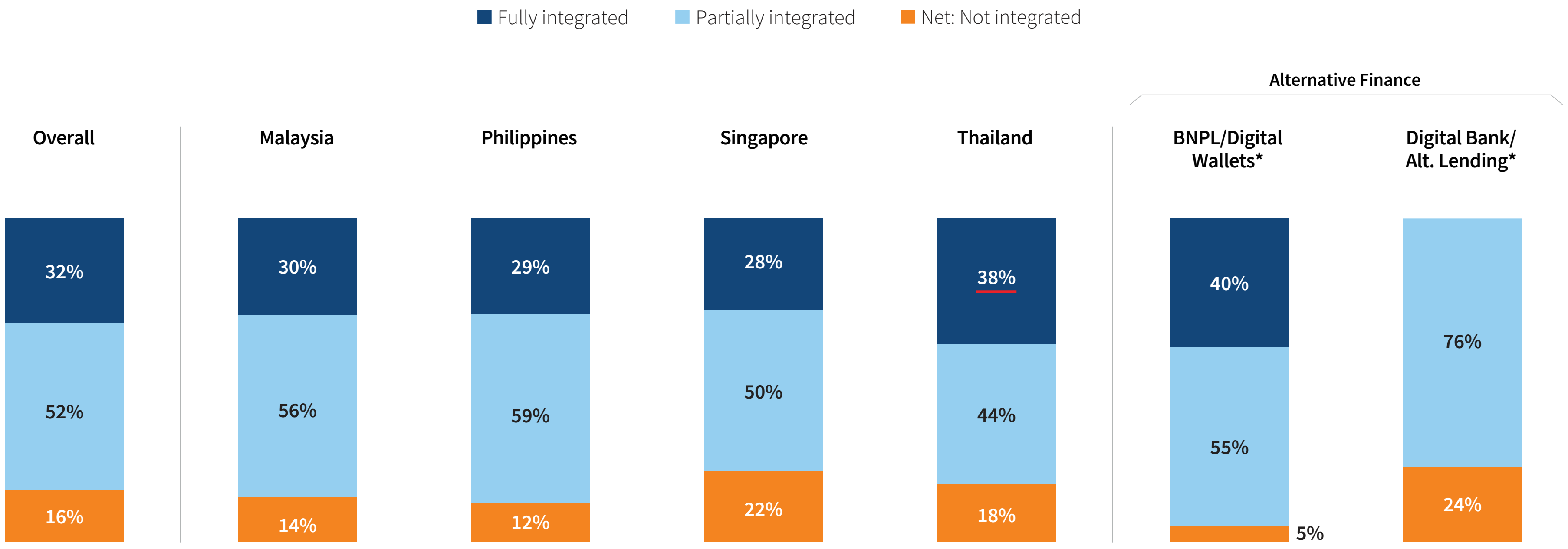
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Few have fully integrated their digital/customer experience operations with fraud prevention, though many are working towards this.

Integration of Digital/Customer Experience Operations w/ Fraud Prevention



— = significantly or directionally higher than same solution in the other customer journey phase

Survey Questions:
Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?
*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

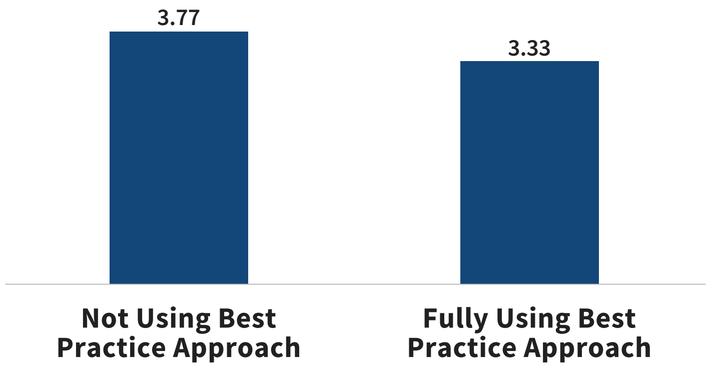
Background & Methodology
Key Findings
Key Finding 01
Key Finding 02
Key Finding 03
Key Finding 04
Key Finding 05
Recommendations
Appendix

KEY FINDING 05

FRAUD DETECTION & PREVENTION APPROACHES

Study findings show that the cost of fraud can be mitigated for organizations that invest in the best practice multi-layered solution approach which is integrated with cybersecurity and digital experience operations.

For every fraudulent transaction among those that implement best practice approaches, the cost is actually 3.33 times the amount of the lost transaction value compared to 3.77 for those not following best practice approaches.



Integration of Cybersecurity, Digital Experience with Fraud Ops	No	Yes
Focus on Optimizing Fraud Risk-to-Friction Levels	No	Yes
Solution(s) to verify physical attributes (e.g., Name, DOB, Address)	✓	✓
Solution(s) to verify digital attributes (e.g., email, phone # risk, biometrics)	Limited or None	✓
Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)	Limited or None	✓
Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)	Limited or None	✓

Survey Questions:
Q30b: To what degree has your company integrated its digital/customer experience operations with its fraud prevention efforts?

*Caution: small sample sizes of N=20 and N=5, respectively (no sig. testing)

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 05

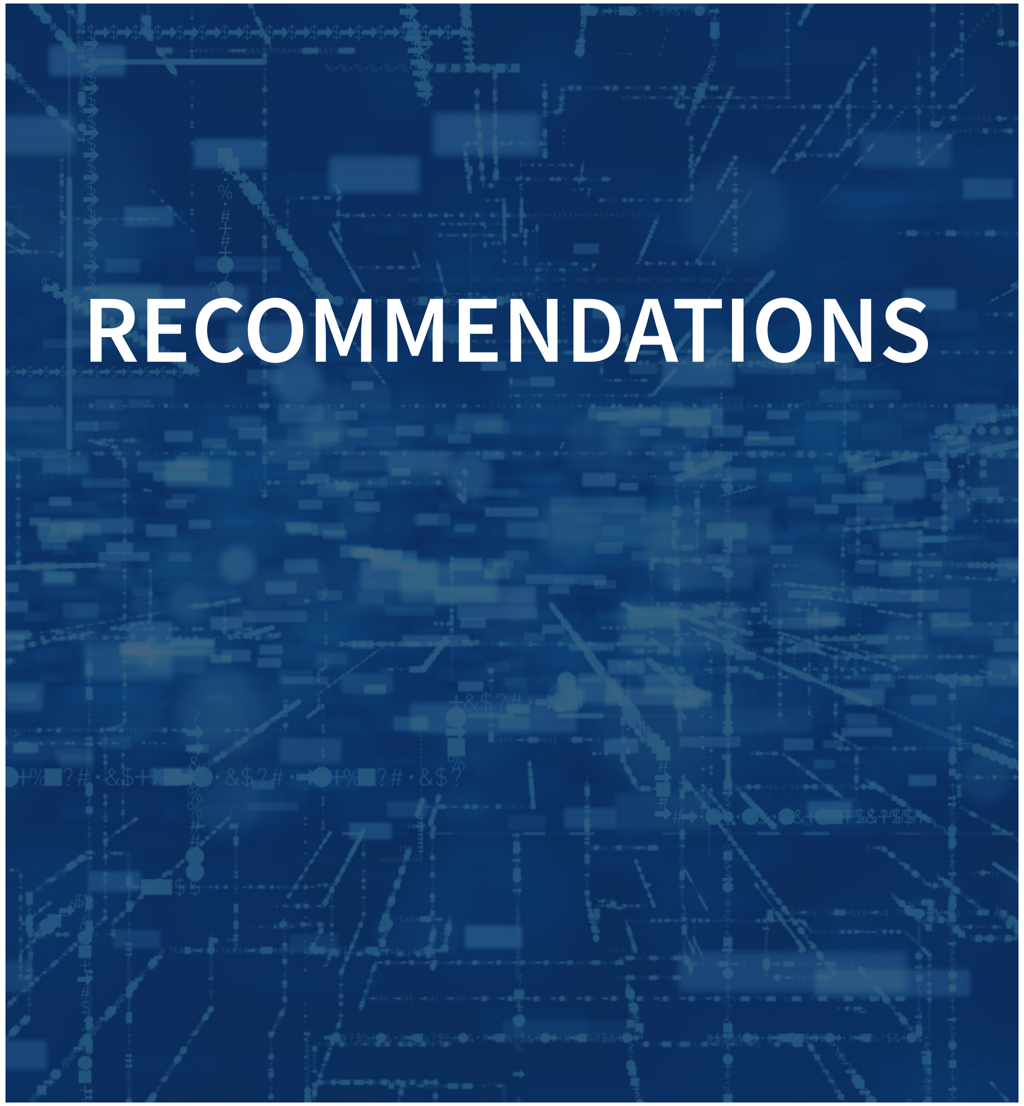
FRAUD DETECTION & PREVENTION APPROACHES

Further, organizations using the best practice multi-layered solution approach report fewer challenges with digital identity verification and the need for manual reviews across customer journey points, particularly with account-related fraud risks.

		Not Using Best Practice Approach		Fully Using Best Practice Approach	
	Integration of Cybersecurity, Digital Experience with Fraud Ops	No		Yes	
	Focus on Optimizing Fraud Risk-to-Friction Levels	No		Yes	
	Solution(s) to verify physical attributes (e.g., Name, DOB, Address)	✓		✓	
	Solution(s) to verify digital attributes (e.g., email, phone # risk, biometrics)	Limited or None		✓	
	Solution(s) to assess device risk, location (e.g., Device ID, Geolocation)	Limited or None		✓	
	Solution(s) to assess behavior (e.g., Behavioral Biometrics, Transaction Risk)	Limited or None		✓	
	% Indicating the Following Challenges at	**Online**	**Mobile**	**Online**	**Mobile**
New Account Creation	Email verification	45%	38%	21%	20%
	Phone # verification	63%	44%	24%	34%
Purchase, Distribution of Funds	Manual reviews	43%	18%	12%	20%
Account Login	Identity verification		43%		28%
	Identity verification	46%	68%	16%	47%
	Email verification	63%		32%	
	Manual reviews	31%		8%	

Best Practice Multi-Layered Solution Approach: Those following a multi-layered solution approach tend to use some combination of passive/digital identity-based solutions and those which assess physical identity attributes and transaction risk.

RECOMMENDATIONS



RECOMMENDATION #1

IDENTITY PROOFING MUST INCLUDE ASSESSING DIGITAL IDENTITY ATTRIBUTES. TECHNOLOGY IS KEY TO THIS EFFORT OF DETECTING AND MITIGATING FRAUD WHILE MINIMIZING FRICTION.

☑ Identity proofing involves both verification and authentication. **Verification** relates to self-provided data (date of birth, national ID number, address, etc.) to determine if the person/identity is real and that the data relates to a single identity; this is particularly important with the rise of synthetic identity fraud. **Authentication** is about confirming that the person is legitimate (who they say they are).

☑ 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.

☑ The digital transformation among consumers to more online and mobile transactions means that more of these transactions are occurring in an anonymous environment compared to traditional in-person interactions. Assessing only the physical identity attributes (name, address, date of birth, Social Security Number, etc.) won’t help businesses authenticate the identity. Businesses need to also assess the device risk, as well as the online/mobile behaviors and transaction risk.

☑ Businesses need a robust fraud and security technology platform that helps them adapt to this 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.

RECOMMENDATION #2

A MULTI-LAYERED SOLUTION APPROACH IS REQUIRED — CUSTOMIZED TO EACH PHASE OF THE CUSTOMER JOURNEY AND TRANSACTION CHANNEL

☑ 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.

☑ Further, each stage of the customer journey is a unique interaction, requiring different types of identity verification, data and solutions to let your customers in and keep the fraudsters out.

☑ 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.

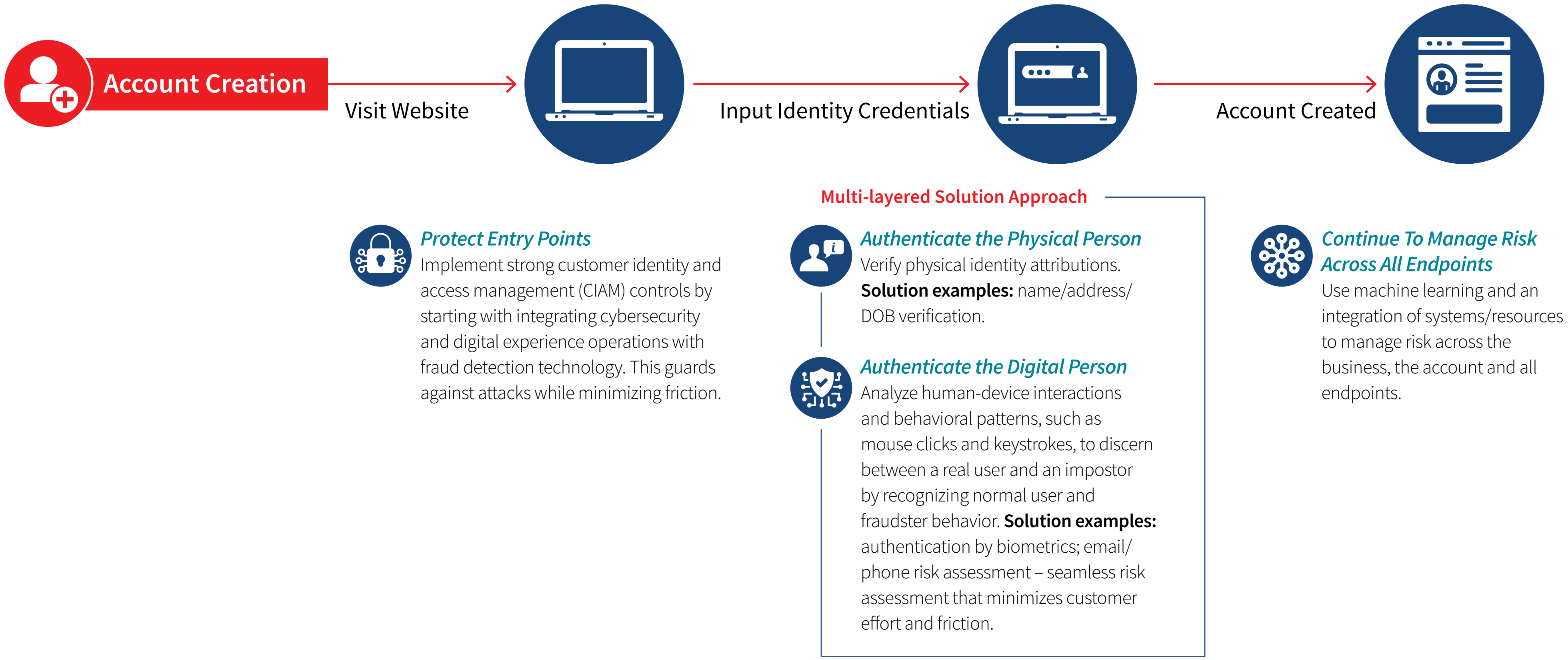
Account Creation → **Account Login** → **Account Transaction**

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

RECOMMENDATION #3

STOP FRAUD AT THE FIRST POINT OF THE CUSTOMER JOURNEY BY PROTECTING ENDPOINTS AND USING DIGITAL IDENTITY SOLUTIONS AND BEHAVIORAL ANALYTICS THAT ASSESS RISK WHILE MINIMIZING FRICTION

New account opening is the customer journey point where fraudsters can become established, causing problems at latter stages. It is also the first point of contact for many legitimate customers; too much friction and they may abandon the effort.



Account Creation → Visit Website → Input Identity Credentials → Account Created

Multi-layered Solution Approach

Protect Entry Points
Implement strong customer identity and access management (CIAM) controls by starting with integrating cybersecurity and digital experience operations with fraud detection technology. This guards against attacks while minimizing friction.

Authenticate the Physical Person
Verify physical identity attributions. **Solution examples:** name/address/DOB verification.

Authenticate the Digital Person
Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment – seamless risk assessment that minimizes customer effort and friction.

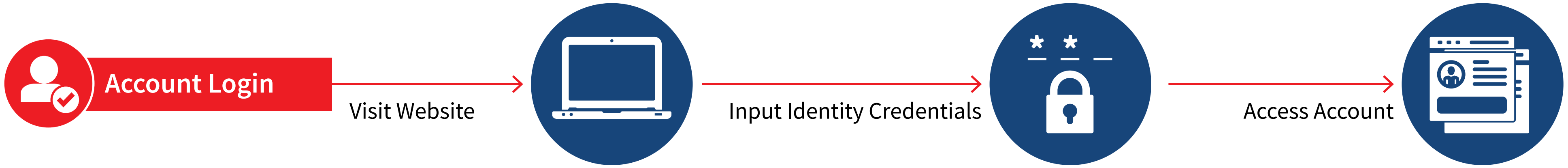
Continue To Manage Risk Across All Endpoints
Use machine learning and an integration of systems/resources to manage risk across the business, the account and all endpoints.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

RECOMMENDATION #4

USE TECHNOLOGIES THAT RECOGNIZE YOUR CUSTOMERS, DETERMINE THEIR POINT OF ACCESS AND DISTINGUISH THEM FROM FRAUDSTERS AND MALICIOUS BOTS. LAYERED SOLUTIONS LET YOU APPLY MORE OR LESS FRAUD ASSESSMENT IN ORDER TO OPTIMIZE THIS WITH THE CUSTOMER EXPERIENCE

Biometrics using fingerprint or facial recognition are particularly useful for account login, based on this information gathered during account creation; this also provides a secure means of identification that speeds the process with minimal friction. Further layering should include device risk assessment to recognize the customer and assess anomalies with location of login. Where anomalies suggest potential risk, authenticate the person through more active ID authentication.



Account Login

Visit Website

Input Identity Credentials

Access Account

Protect Entry Points

Implement strong customer identity and access management (CIAM) controls by starting with integrating cybersecurity and digital experience operations with fraud detection technology. This guards against attacks while minimizing friction.

Breached data used to access accounts requires more levels of security and authentication of the person from a bot or synthetic identity.

Multi-layered Solution Approach

Authenticate the Digital Person to Distinguish Between Legitimate and Fake Customers/Fraudsters

Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior.

This is particularly important at account login since fraudsters deploy mass bot attacks, using breached data, to test passwords for account takeover.

Synthetic identities involve real and fake identity data. Physical identity attribute assessment alone will not make this distinction.

Solution examples: authentication by biometrics; email/phone risk assessment – seamless risk assessment that minimizes customer effort and friction.

Authenticate the Device

Identify a remote computing device or user. **Solution examples:** device ID/fingerprint; geolocation.

Active Identity Authentication

Use personal data known to the customer for authentication; or where a user provides two different authentication factors to verify themselves. **Solution examples:** authentication by challenge, quiz or shared secrets; authentication using OTP/ 2 factor.

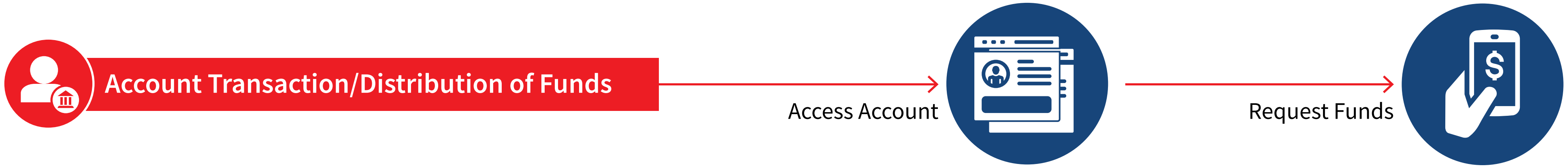
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

RECOMMENDATION #5

ADD TRANSACTION RISK TECHNOLOGY TO THE LAYERING OF DIGITAL ATTRIBUTES, BEHAVIORAL ANALYTICS AND DEVICE ASSESSMENT SOLUTIONS DURING THE TRANSACTION/DISTRIBUTION OF FUNDS JOURNEY POINT

As consumers transact across locations, devices and geographies, their behaviors, such as transaction patterns, payment amounts and payment beneficiaries, are becoming more varied and less predictable.



Multi-layered Solution Approach

Authenticate the Digital Person
Analyze human-device interactions and behavioral patterns, such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment – seamless risk assessment that minimizes customer effort and friction.

Authenticate the Device
Identify a remote computing device or user. **Solution examples:** device ID/fingerprint; geolocation.

Active Identity Authentication
Use personal data known to the customer for authentication; or where a user provides two different authentication factors to verify themselves. **Solution examples:** authentication by challenge, quiz or shared secrets; authentication using OTP/ 2 factor.

Assess the Transaction Risk
Velocity checks/transaction scoring: Monitor historical transaction patterns of an individual against their current transactions to detect if volume by the cardholder matches up or if there appears to be an irregularity. **Solution examples:** real-time transaction scoring; automated transaction scoring.

APPENDIX

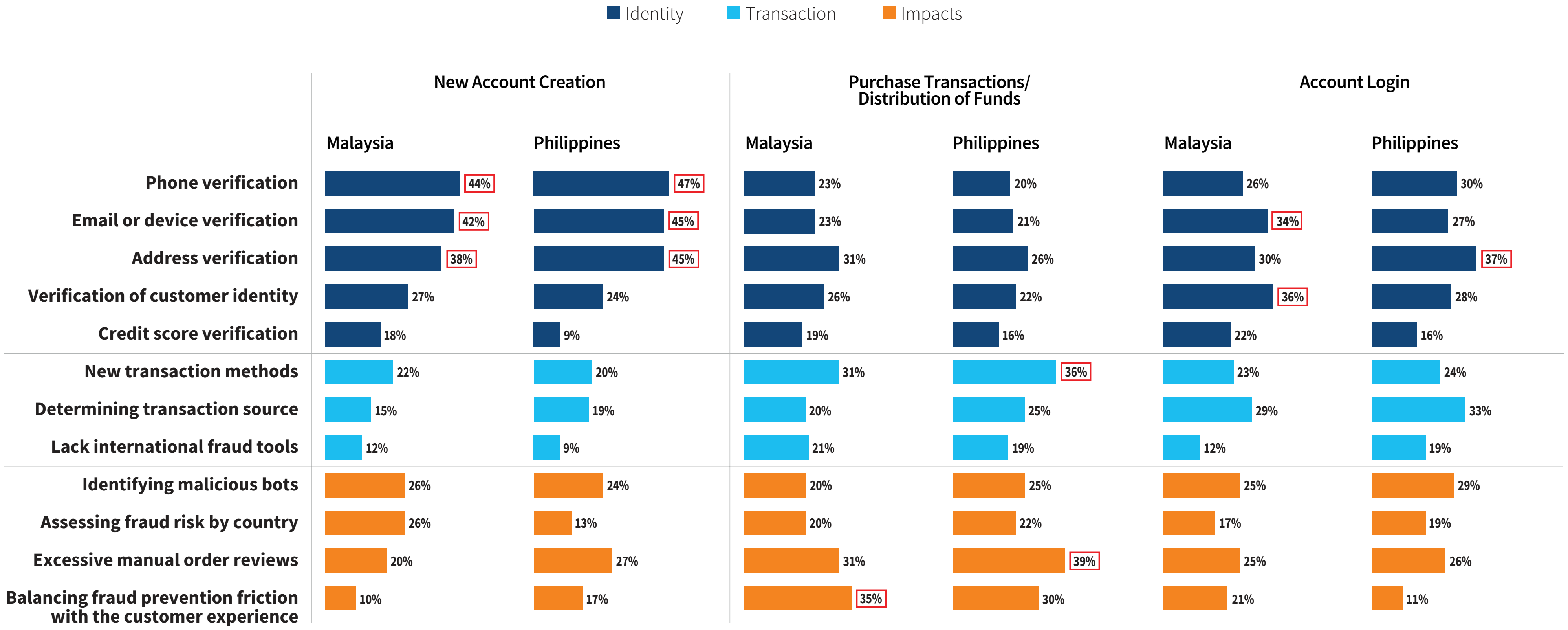
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

Online Fraud Challenges by Country Across the Customer Journey

Top Three Ranked ONLINE Fraud Challenges



☐ = significantly or directionally higher than most or all other challenges within customer journey phase

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online channel.

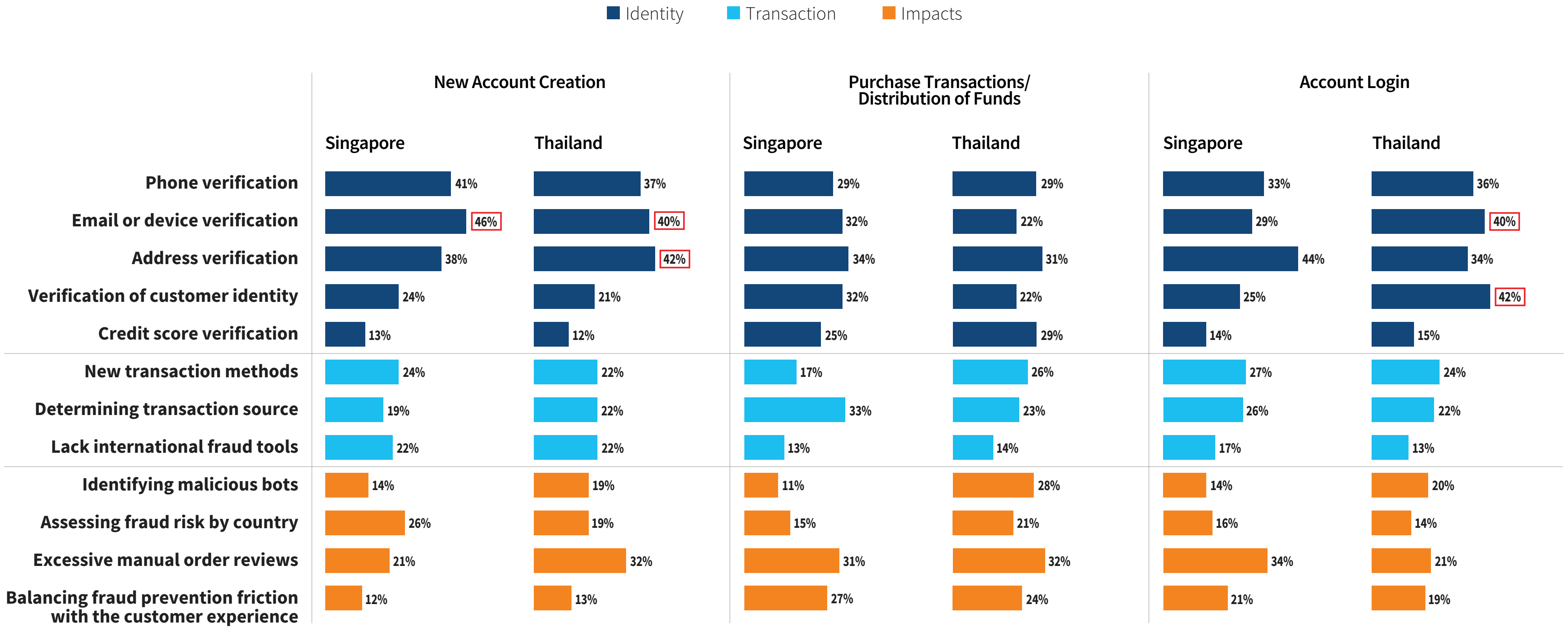
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

Online Fraud Challenges by Country Across the Customer Journey

Top Three Ranked ONLINE Fraud Challenges



☐ = significantly or directionally higher than most or all other challenges within customer journey phase

Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online channel.

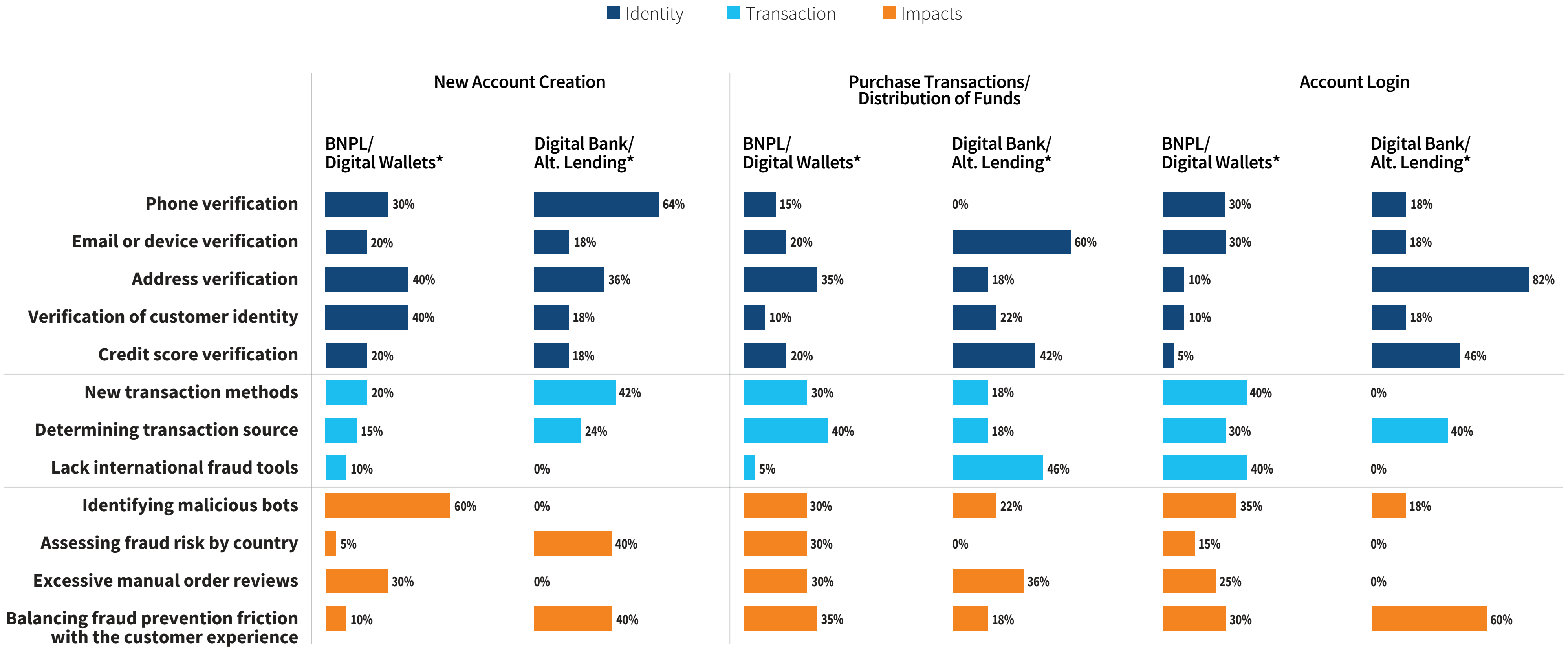
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY ONLINE CHANNEL CHALLENGE

Online Fraud Challenges by Alternative Finance Across the Customer Journey

Top Three Ranked ONLINE Fraud Challenges



Survey Questions:
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the online channel.

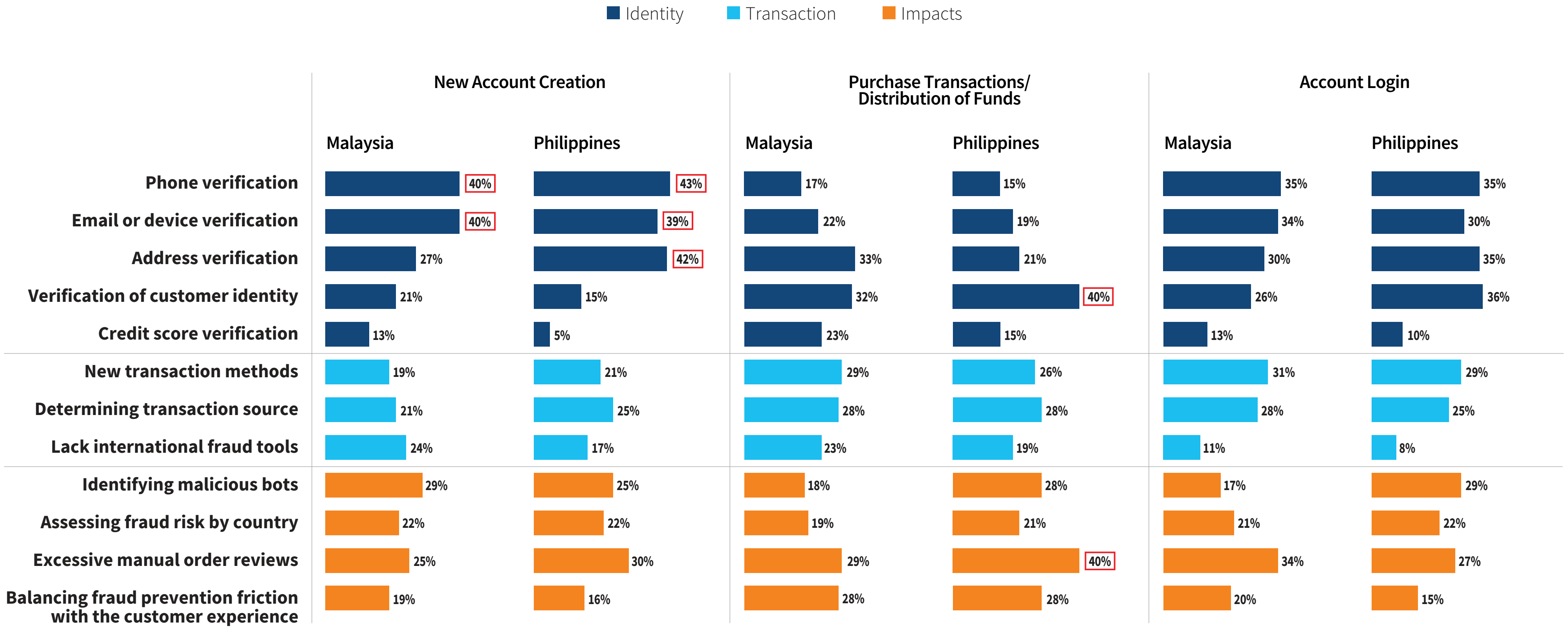
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

Mobile Fraud Challenges by Country Across the Customer Journey

Top Three Ranked MOBILE Fraud Challenges



☐ = significantly or directionally higher than most or all other challenges within customer journey phase

Survey Questions:
Q20b: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the mobile channel.

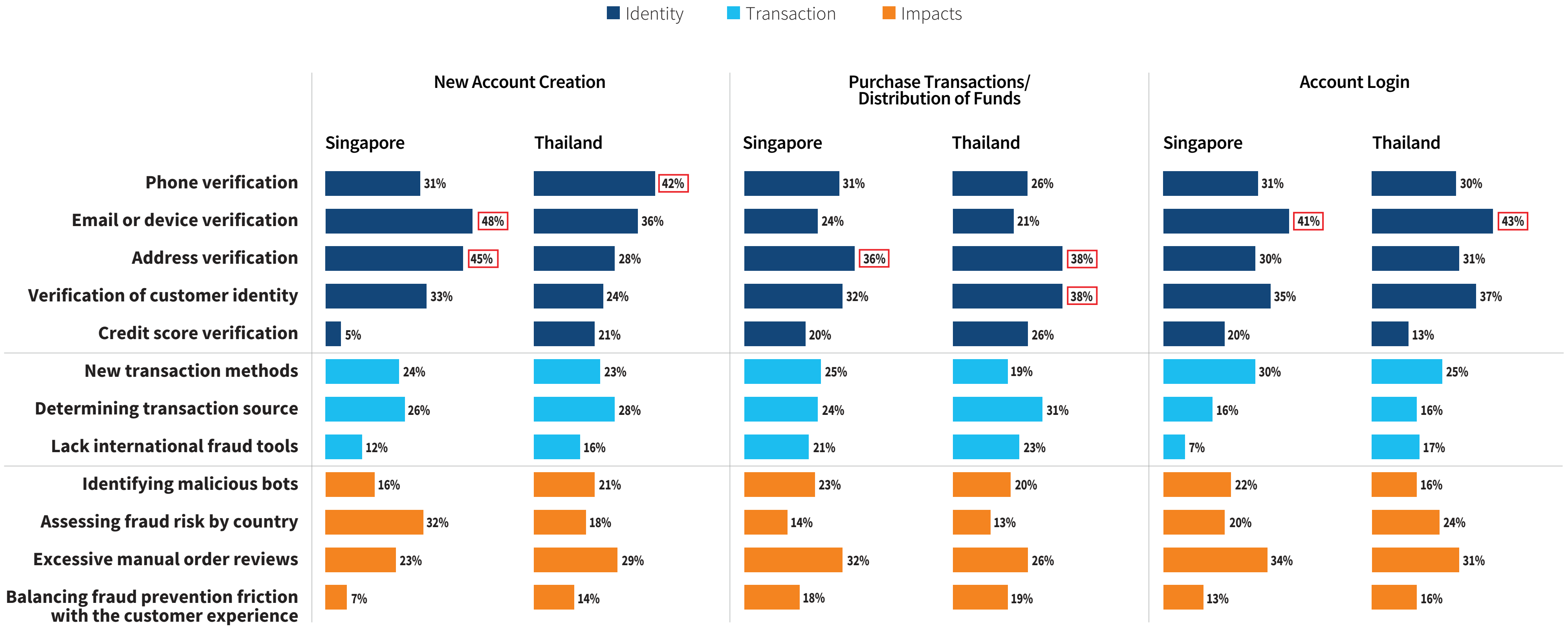
COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

Mobile Fraud Challenges by Country Across the Customer Journey

Top Three Ranked MOBILE Fraud Challenges



☐ = significantly or directionally higher than most or all other challenges within customer journey phase

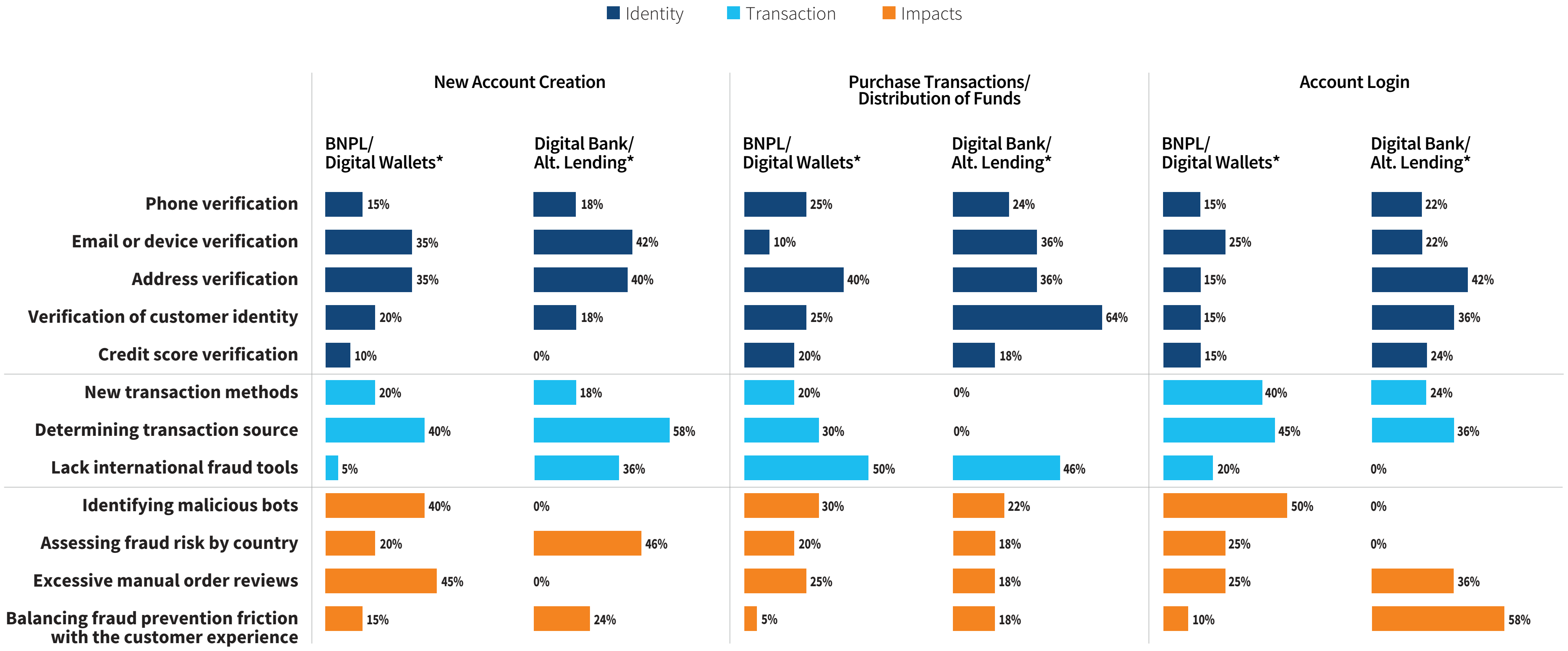
Survey Questions:
Q20b: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the mobile channel.

KEY FINDING 04

IDENTITY VERIFICATION AS A KEY MOBILE CHANNEL CHALLENGE

Mobile Fraud Challenges by Alternative Finance Across the Customer Journey

Top Three Ranked MOBILE Fraud Challenges



Survey Questions:
Q20b: Please rank the top 3 challenges related to fraud faced by your company when serving customers using the mobile channel.

COPYRIGHT © 2022 LEXISNEXIS RISK SOLUTIONS

LEXISNEXIS® RISK SOLUTIONS CAN HELP CREATE THE BEST CUSTOMER EXPERIENCE, UNDERPINNED BY MULTIPLE LAYERS OF DEFENSE

Shared intelligence network

1st

Digital Identity Assessment

- Customer identity data
- Identity resolution, attributes & anomalies
- Web & mobile device intelligence
- True geolocation, VPN, proxies & TOR
- Behavioral analytics
- Malware & bot threat intelligence

2nd

Decision Analytics

- Industry best practices & decision policies
- Identity correlation & linkages
- Behavioral analytics & variables
- Machine learning
- Integration & orchestration

3rd

Authentication

- Strong ID
- Push Authentication
- Behavioral Biometrics
- Document Authentication
- SMS/Voice Authentication
- OTP

4th

Digital Identity Assessment

- Forensics & investigation
- Case management & workflow
- Reporting
- Feedback, audit & policy governance

LexisNexis®
RISK SOLUTIONS

For more information:
risk.lexisnexis.com/CNP-FIM-EN

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/ NYSE: RELX), a global provider of information-based analytics and decision tools forprofessional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

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. LexisNexis Fraud Multiplier is a service mark of RELX Inc. True Cost of Fraud is a service mark of LexisNexis Risk Solutions Inc. Copyright © 2022 LexisNexis Risk Solutions