LexisNexis® Risk Solutions 2021 True Cost of Fraud™ APAC Study

INDIA REPORT

MAY 2021

LexisNexis®
RISK SOLUTIONS

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 market retail, e-Commerce, financial services, and lending markets.
- Key pain points related to adding new payment mechanisms, transacting though online and mobile channels, and expanding internationally.

COVID-19 Impact:

- Data collection occurred during February – April 2021; 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 behaviours 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 total amount of loss a firm occurs based on the actual dollar value of a fraudulent transaction

BACKGROUND & METHODOLOGY

The study included a comprehensive survey of 418 risk and fraud executives in Retail and e-Commerce companies as well as Financial Services and Lending, in the APAC region. This report presents findings for the Indian market.

	Australia	Hong Kong	India	Japan
Retail	40	42	47	38
e-Commerce	32	33	31	31
Financial Services	31	33	30	30
TOTAL	103	108	108	99

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
Asset Management
Banking / Mortgage
Consumer Lending
Financial Planning

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*

SUMMARY OF KEY FINDINGS

1. **The cost of fraud for surveyed industries in India is 3.84 times the lost transaction value on average. It is higher among financial services institutions,** as fraud attempts at phishing and stealing of bank account information heightened during the COVID-19 pandemic.

2. **There is increased digital transaction and digital payment activity occurring in India – at least in Tier I and Tier II areas, given the COVID-19 pandemic. This is occurring through both the online/web browser and mobile channels, adding to fraud risks and costs.** While smartphone penetration is lower that other markets across the population as a whole, there are just over 425 million subscribers – largely in the urbanised areas that are driving use of mobile browsers and apps. Mobile/digital wallets are on par with credit and debit card payment methods, largely resulting from a movement away from cash and in-person transactions given fear of virus transmission.

3. **Identity-related fraud is a key threat and challenge for Indian retail/E-commerce merchants and financial institutions.** This relates specifically to remote transaction channels where more real-time transaction tracking and data is needed to fight synthetic identities and bot attacks. For E-commerce merchants, there is added difficulty determining order location/transaction origination, distinguishing between legitimate and bot-related transactions and dealing with new payment methods.

4. **Merchants and financial services firms that use a multi-layered approach involving passive/digital/transaction risk mitigation solutions that are integrated with their cybersecurity and digital customer experience can more effectively detect and prevent fraud, minimise customer friction and lower their cost of fraud.** Currently, only a few Indian merchants and financial institutions are using this best-practice.

KEY FINDING 01

The cost of fraud for surveyed industries in India is 3.84 times the lost transaction value on average. It is higher among financial services institutions.

The cost of fraud is 4.76 times the lost transaction value for financial services institutions compared to retail and E-commerce merchants.

There has been increased fraud directed particularly at E-commerce and financial services firms involving phishing and stealing of bank account information. Financial services firms are at more risk given more international transactions and being the payment source for fraud directed at retailer/E-commerce merchants.

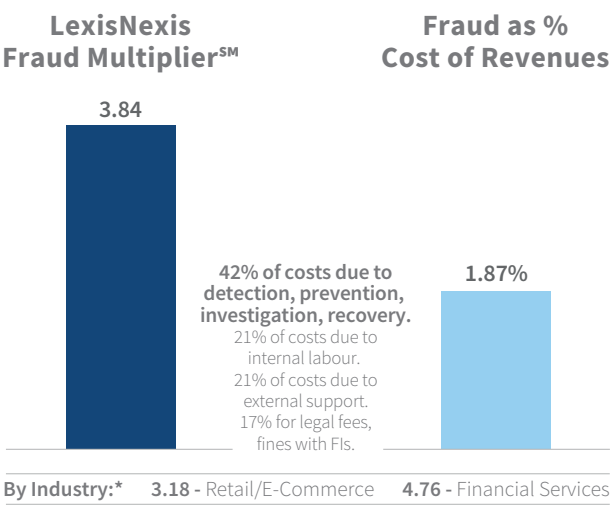
KEY FINDING 01
FRAUD COSTS & VOLUME

The LexisNexis Fraud Multiplier℠ is 3.84 across surveyed industries in India, though differs significantly between merchants and financial institutions.

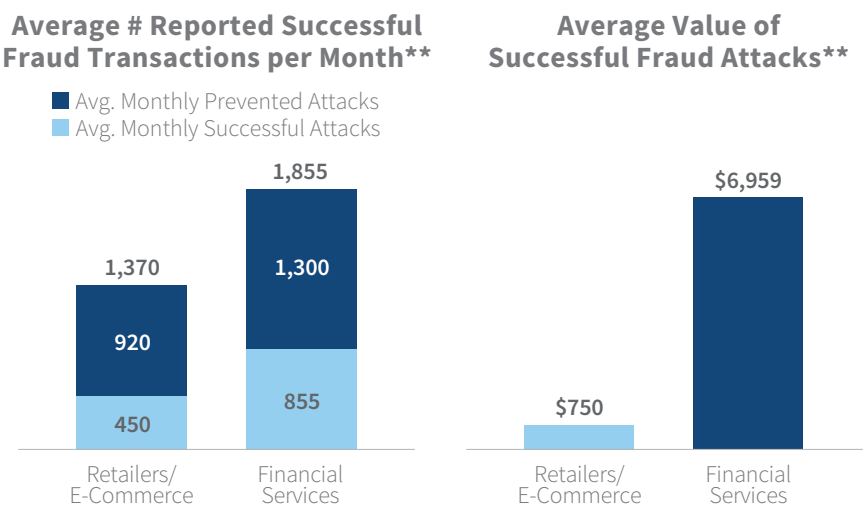
For every fraudulent transaction, the cost to Indian retail/E-commerce merchants is 3.18 times the amount of the lost transaction value. For financial institutions, it is a multiplier of 4.76. FIs face fraud impacts on two fronts: 1.) indirectly through chargebacks submitted by retailers hit with fraud; and, 2.) fraud attacks targeted directly at them.

There has been increased fraud directed at Indian banks and E-commerce merchants, including more digital-based fraud during COVID-19 involving online banking and fraudulent E-commerce sites phishing for/stealing bank account details.[1,2,3] This has been specifically illustrated through QR code scams to obtain UPI payment details (Unified Payments System of real-time payment transfers).[4,5]

Cost of Fraud: LexisNexis Fraud Multiplier™



Average Volume / Value of Total Fraud Attempts Per Month



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?
Q22/24: In a typical month, approximately how many fraudulent transactions are prevented/successfully completed by your company?
Q23/25: What is the average value of such a transaction?

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

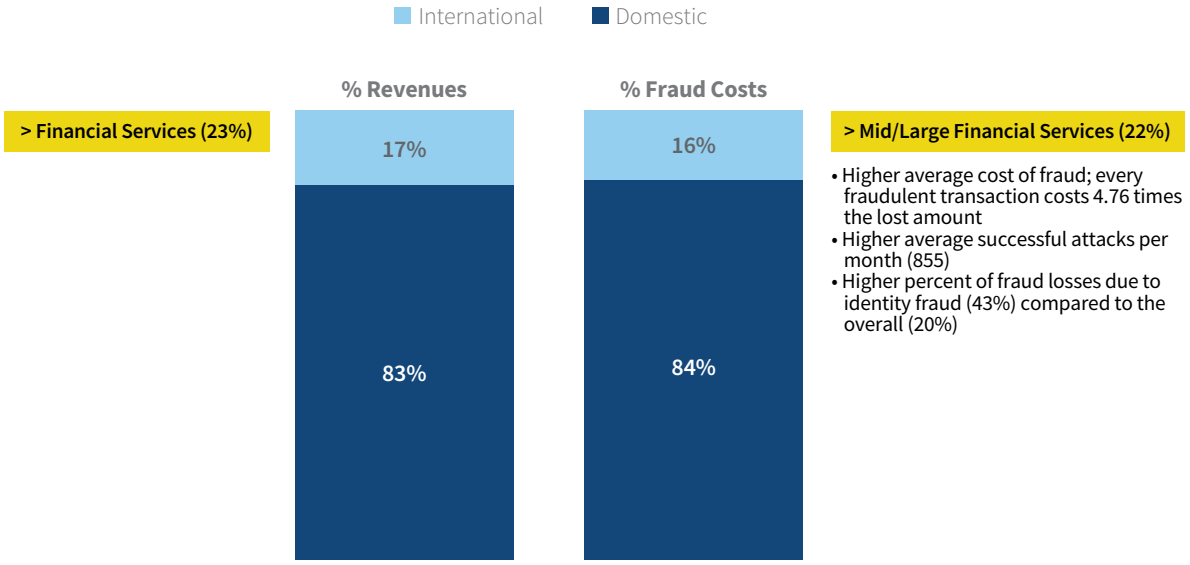
1 https://www.mondaq.com/hongkong/white-collar-crime-anti-corruption-fraud/997778/cyber-fraud-and-recovery-in-hong-kong
2 https://www.newindianexpress.com/cities/thiruvananthapuram/2020/jun/25/extended-lockdown-sees-spike-in-online-fraud-2160883.html
3 https://www.securitymagazine.com/articles/92932-heightened-fraud-and-cyber-risks-threaten-e-commerce-merchants
4 https://indianexpress.com/article/technology/opinion-technology/what-is-qr-code-phishing-and-how-to-protect-yourself-from-it-7174553/
5 https://indianexpress.com/article/cities/delhi/cyber-crime-rose-during-lockdown-7196262/

KEY FINDING 01
FRAUD COSTS & VOLUME

Major revenue and fraud losses come from Indian-based transactions, though international increases fraud risks and costs.

Where there is international-related fraud, it is directionally more so among financial institutions that report a larger share of non-domestic business. This increases their risk of fraud attacks and associated higher costs, including more successful attacks per month and a higher portion of those related to identity fraud compared to others.

Domestic vs. International Transactions & Fraud Costs



Survey Questions:
Q9/13: Please indicate the percent of annual revenue/fraud costs generated through domestic compared to international transactions in the last 12 months

KEY FINDING 02

There is increased digital transaction and digital payment activity occurring in India, given the COVID-19 pandemic. This is occurring through both the online/ web browser and mobile channels, adding to fraud risks and costs.

At least in Tier I and Tier II areas, more online and mobile transactions are occurring for both shopping and banking.

- With this, there is a higher volume of transactions involving mobile wallets and debit cards compared to the regional 2019 average; volume for both of these methods is on par with credit cards, while transactions involving cash are significantly below regional 2019 averages.
- Not surprisingly, these digital payment methods account for more fraud losses than other methods.

Mobile browsing and app use is common for mobile channel transactions. While smartphone penetration is lower in India based on the total population, it nonetheless involves a significant number of consumers (over 425 million), predominantly in the Tier 1 and Tier II areas. Top providers such as Flipkart, Tata and Amazon India have been pushing mobile apps use.

Online/Web browsers account for the single largest source of fraud (41%), though the mobile channel accounts for over one-quarter (27%), with mobile browsers and apps contributing the bulk of this.

Identity-related fraud is particularly troubling for financial institutions, representing just under half (43%) of fraud losses; this is just under double the level compared to retail/E-commerce merchants. Account takeover fraud also represents more fraud losses among financial institutions compared to retail/E-commerce.

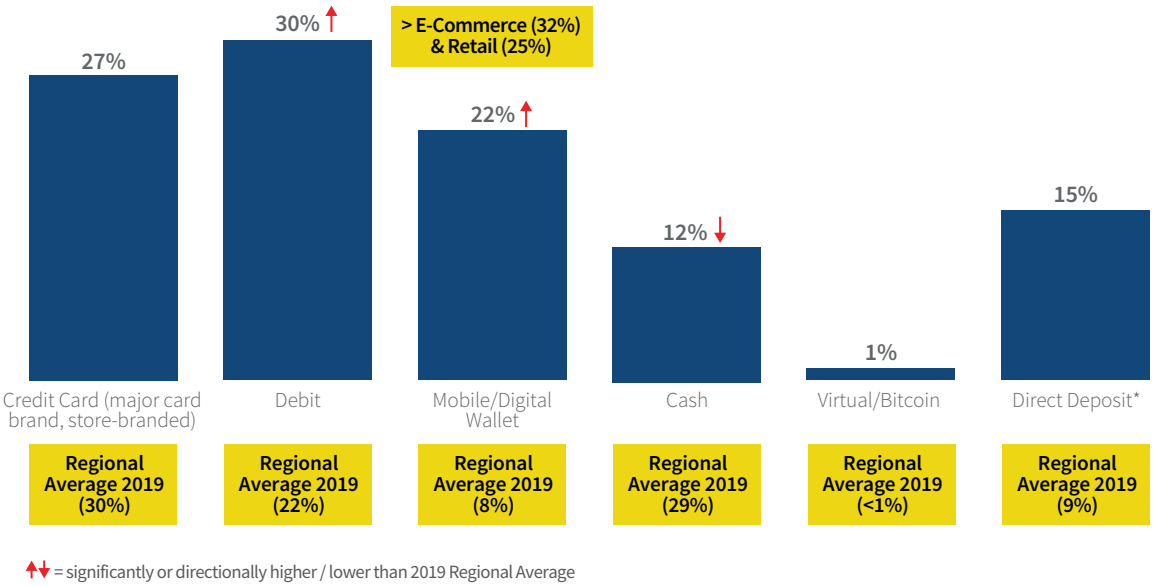
KEY FINDING 02
FRAUD TRENDS

As COVID-19 impacted everything during the past 12 months, more transactions have involved digital payment methods instead of cash.

Compared to the 2019 Regional average, the percent of transactions involving debit cards and mobile/digital wallets has increased significantly while cash transactions dropped significantly.

While India is very cash-transaction and cash-on-delivery oriented, fear of the virus has driven a surge in digital payments during the past 12 months.[6, 7, 8] In fact, the Coronavirus has been more successful at moving people from cash to digital payments than the government's demonetization program launched in late 2016, with recent studies indicating a majority of Indian consumers – at least in Tier 1 and Tier 2 areas - using digital payments since the virus outbreak.[9]

Average Distribution of Transaction Volume Across Payment Methods



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.

*Asked only of Financial Institutions

6 https://retail.economictimes.indiatimes.com/news/e-commerce/e-tailing/e-commerce-revolution-in-india-gets-its-second-wind-post-covid-19/77460376
7 https://www.financialexpress.com/industry/digital-payments-jump-135-during-fy18-20-upi-cards-see-highest-volume/2103051/
8 https://insync.co.in/the-growth-in-mobile-commerce-in-2020-impact-of-coronavirus/
9 https://theprint.in/economy/coronavirus-succeeds-where-demonetisation-failed-as-indians-dump-cash-for-digital-payments/459599/

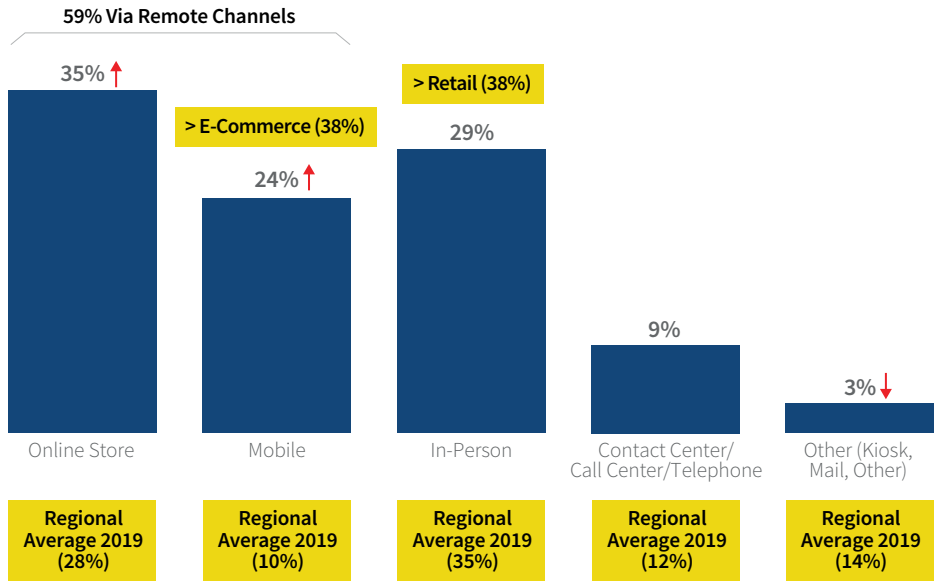
KEY FINDING 02
FRAUD TRENDS

Not surprisingly, digital channels are being used for transactions more often as a result of COVID-19, though in-person retail still represents a sizeable portion.

As in other global markets, in-person transactions and fear of COVID-19 have moved many people towards online or mobile channel transactions. And, just prior to the pandemic, a study by a major payments provider showed that just over half of online sales in India came from mobile devices (i.e., M-commerce) which aligns with other reporting of M-commerce accounting for nearly half (49%) of E-commerce transactions.[10, 11]

Digital transactions are not exclusive to shopping. There has been growth with digital banking, with more than 332 million people having established mobile phone banking accounts as of 2019, based on the government's Jan-Dhan Yojana mass financial-inclusion programme.[12] Overall, India is seen as digitizing faster than any other markets except Indonesia.[13]

Average Distribution of Transaction Volume Across All Channels



↑↓ = significantly or directionally higher / lower than 2019 Regional Average

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.

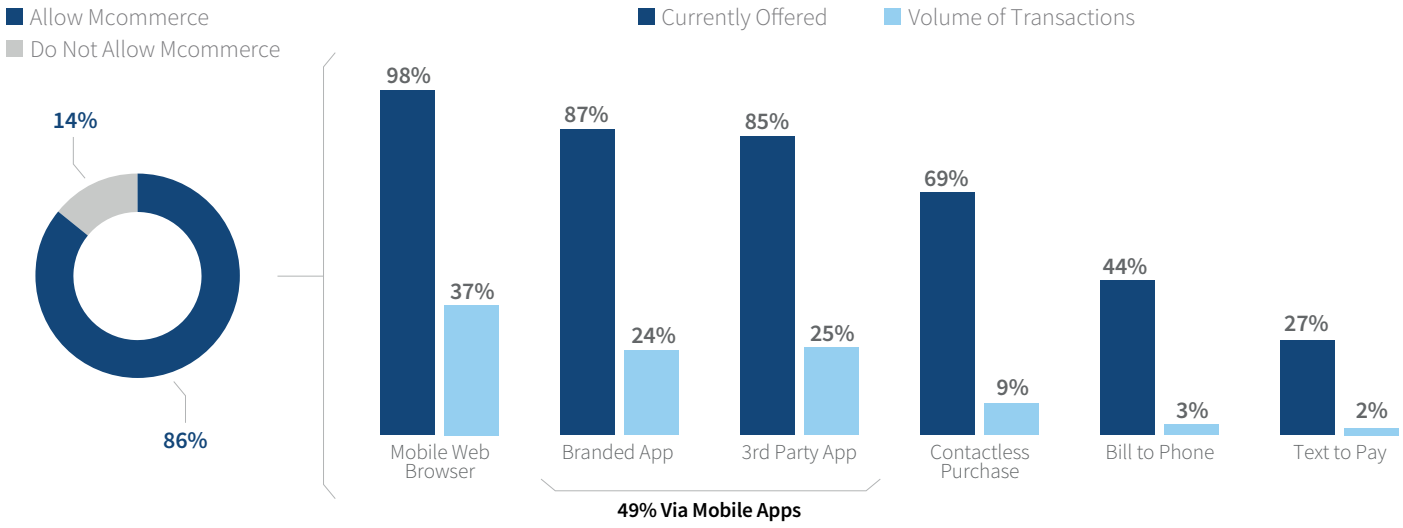
10 https://insync.co.in/the-growth-in-mobile-commerce-in-2020-impact-of-coronavirus/
11 https://www.jpmorgan.com/merchant-services/insights/reports/india-2020
12 McKinsey Global Institute, Digital India, March 2019; https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.pdf
13 Ibid

KEY FINDING 02
FRAUD TRENDS

As in other markets, mobile browser and apps represent the majority of transactions made through this channel.

Amazon India, Flipkart and Tata are key providers pushing mobile apps use, especially in the pandemic-restricted environment.[14] That said, while smartphone penetration is growing in India, it still remains low as a percentage of the population (31.8%)[15] – though involves a very high number of people (over 425 million).[15]

Businesses Offering M-Commerce



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.

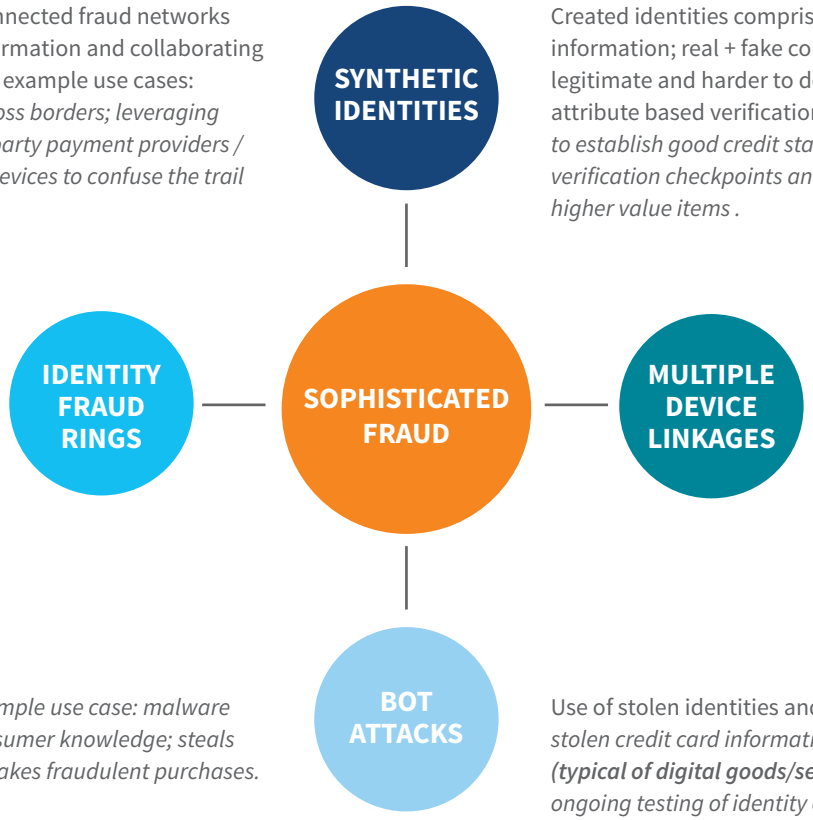
14 https://www.jpmorgan.com/merchant-services/insights/reports/india-2020
15 Statista
16 McKinsey Global Institute, India's Turning Point, August 2020; https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/India/Indias%20turning%20point%20An%20economic%20agenda%20to%20spur%20growth%20and%20jobs/MGI-Indias-turning-point-Report-August-2020-vFinal.pdf

KEY FINDING 02
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 m-commerce.

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.



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.*

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 .*

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.*

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.*

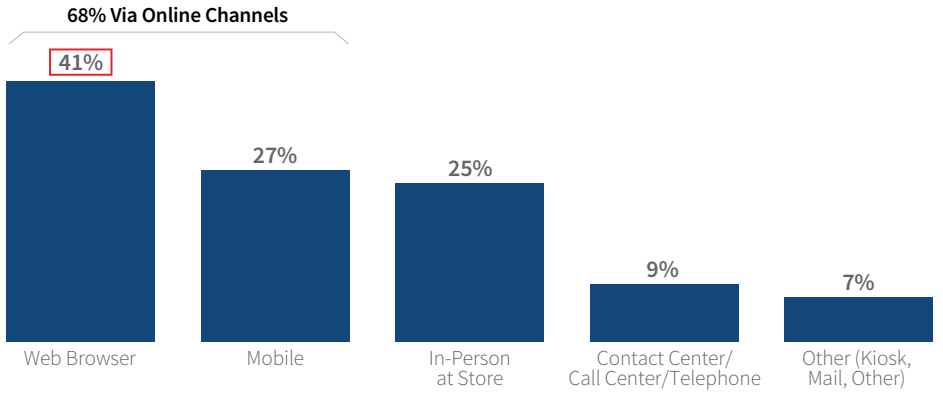
KEY FINDING 02
FRAUD TRENDS

A significant share of fraud costs come from remote channels.

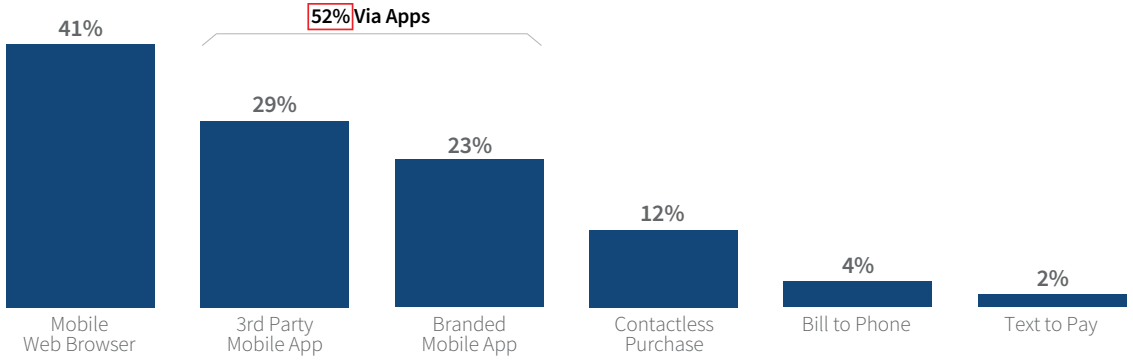
The web browser channel accounts for the single largest source of fraud costs in India.

As would be expected, the primary mobile transaction methods (mobile browser, mobile apps) account for the majority of fraud costs in the mobile channel. 3rd party mobile apps are linked to more fraud costs than companies' own branded apps.

% Fraud Costs by Channel*



% Fraud Costs by Mobile Channel*



Survey Questions:
Q15. Please indicate the percent of fraud costs generated through each of the following transaction channels used by your company.
Q17. Please indicate the distribution of fraud across the various mobile channels you use/accept..

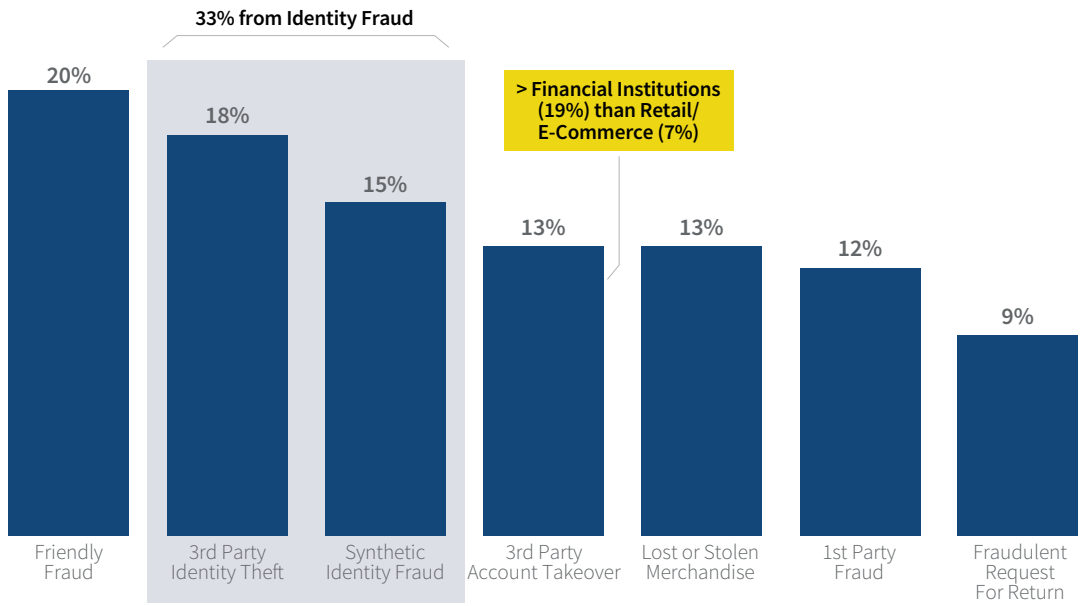
☐ = significantly or directionally higher than most or all other categories

KEY FINDING 02
FRAUD TRENDS

Identity fraud represents a significant portion of Indian financial institutions' fraud losses, nearly double the level for retailers / E-commerce merchants.

This likely relates to the cybercrime scams targeting access to bank accounts, especially since financial institutions also attribute a similar distribution of fraud losses to account takeover as they do to 3rd party and synthetic identity fraud individually – and significantly more so compared to retail and E-commerce merchants.

% Distribution of Losses by Fraud Type



Identity Fraud

Greater distribution of fraud losses among:

- Financial institutions (43%) than retail / E-commerce (22%)

Survey Questions:
Q12a: Now, please think about your total fraud loss over the past 12 months. Please indicate the percentage distribution of the following fraud methods, as they are attributed to your fraud losses that occurred during the past 12 months. Please estimate to the best of your knowledge.
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

KEY FINDING 02
FRAUD TRENDS

Account-related fraud represents a sizeable portion of identity-related fraud losses.

Identity-Related Fraud: % Distribution by Activity*

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

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

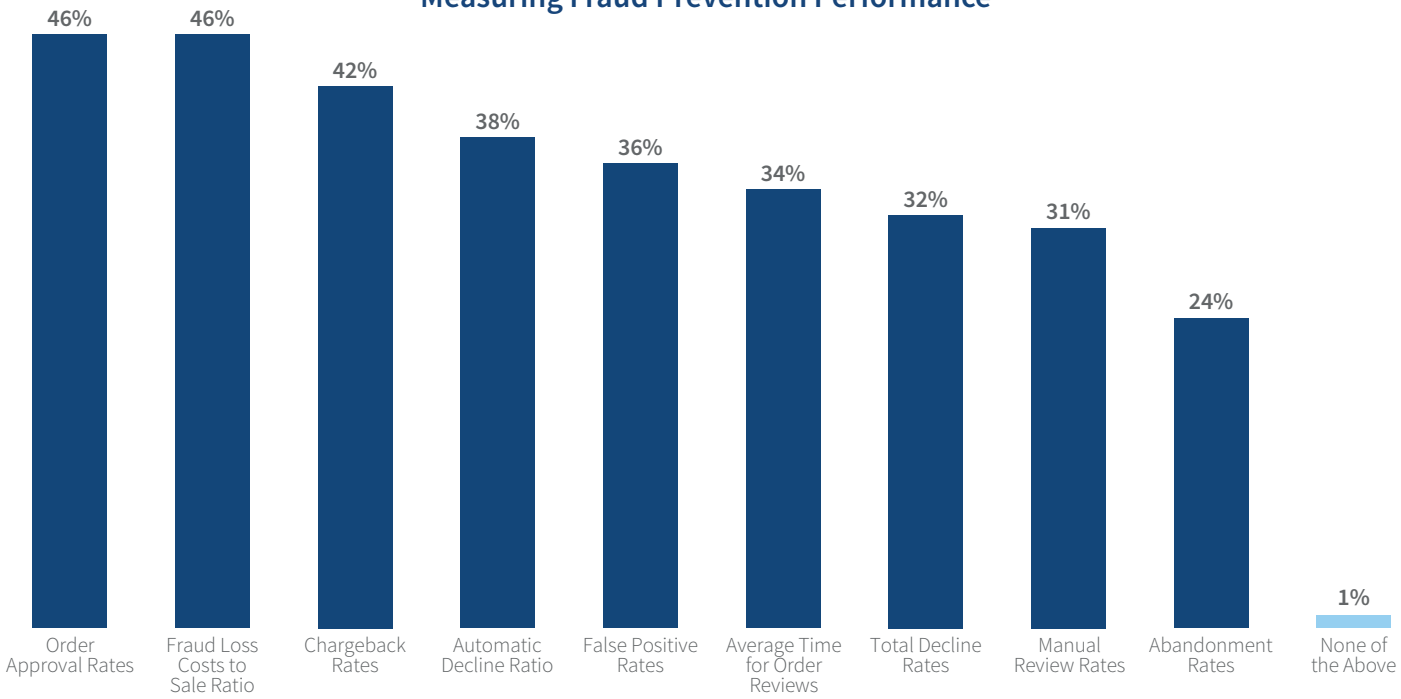
* Caution low base size

KEY FINDING 02
FRAUD TRENDS

Fraud performance metrics vary. Organisations focused on minimizing customer friction at point of transaction are more likely than others to use metrics that assess speed and approval/decline rates. But, fewer overall are assessing abandonment rates.

It is important to assess speed and approval/decline rates. However, those that are not measuring fraud prevention by abandonment rates are missing key data that relates directly to reasons for abandonment (customer friction).

Measuring Fraud Prevention Performance



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

Organisations focused on minimizing customer friction at the point of transaction are more likely than others (not focused on minimizing friction) to use the following metrics:

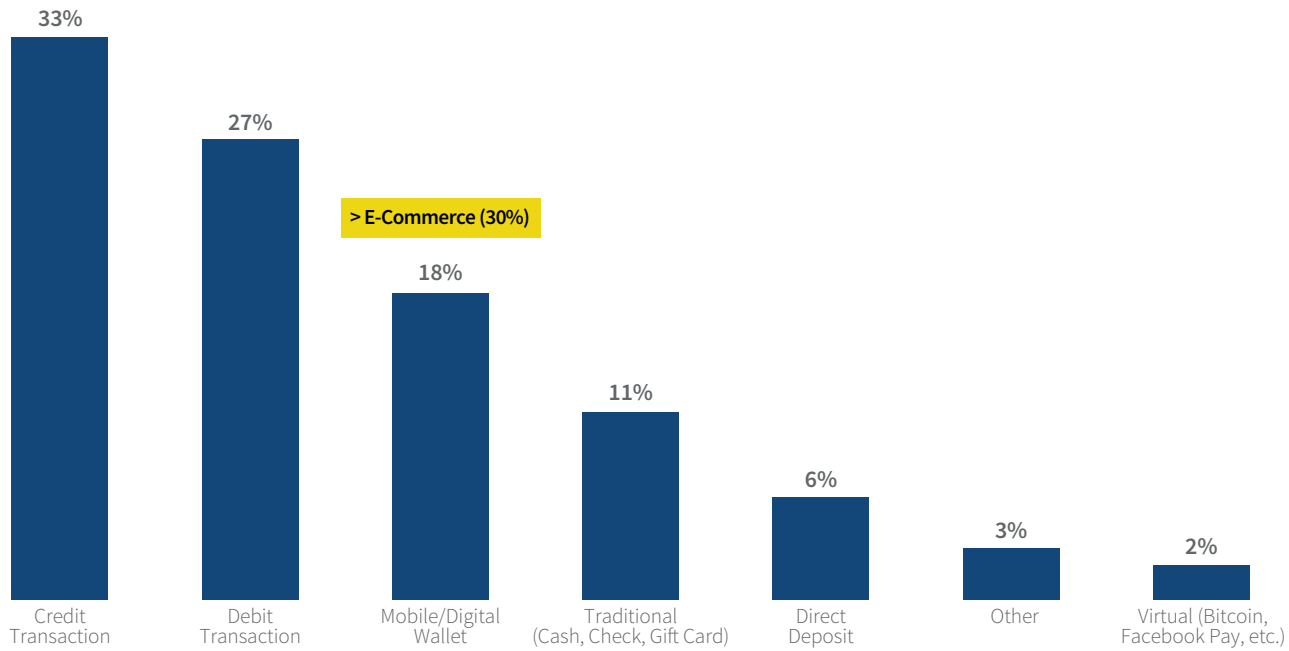
- Order approval rates (58% vs. 40%)
- Average time for order reviews (49% vs. 26%)
- Automatic decline rates (50% vs. 33%)
- Abandonment rates (33% vs. 20%)

KEY FINDING 02
FRAUD TRENDS

Card-based transactions account most fraud losses by payment method, though mobile / digital wallets represent a sizeable portion of E-commerce losses as well.

The rise of mobile / digital wallets can pose fraud risks to merchants and financial institutions if breached card data is used during card enrollment process, therefore the need for strong authentication processes and tools.

% Distribution of Losses by Payment Method

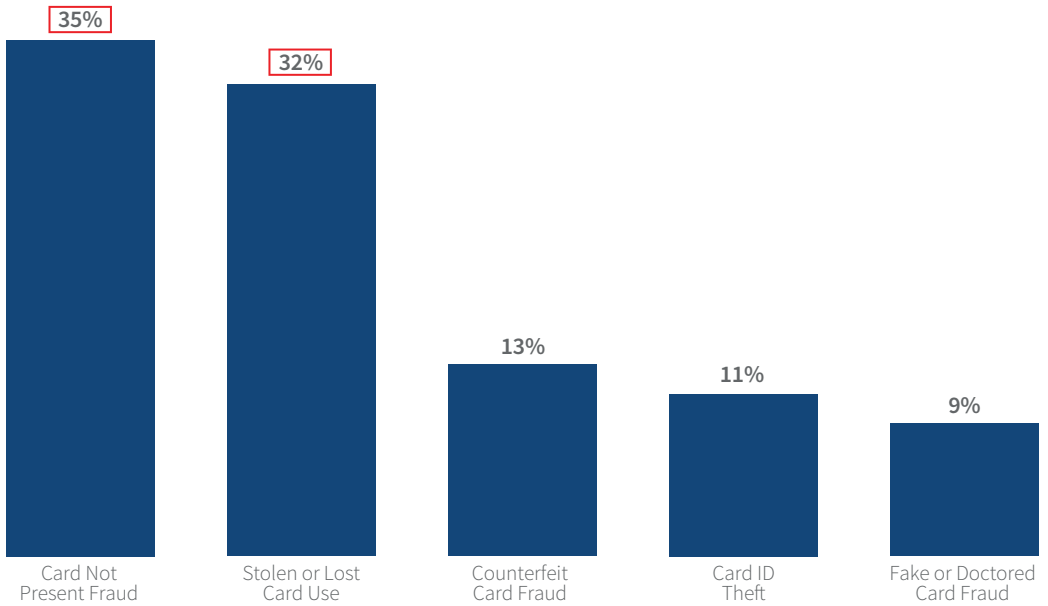


Survey Questions:
Q18: In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of fraud costs for each of the payment methods.

KEY FINDING 02
FRAUD TRENDS

Card-not-present (CNP) and stolen / lost cards contribute most to card-related fraud losses.

% Distribution of Card-Related Fraud Losses



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

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

KEY FINDING 03

Identity-related fraud is a key threat and challenge for Indian retail/E-commerce merchants and financial institutions.

Identity-related fraud is a key challenge for online/browser and mobile channel transactions, with new mobile payment methods contributing to this. For E-commerce merchants, these challenges are heightened by the difficulty of determining order location / transaction origination, distinguishing between legitimate and bot-related transactions and dealing with new payment methods.

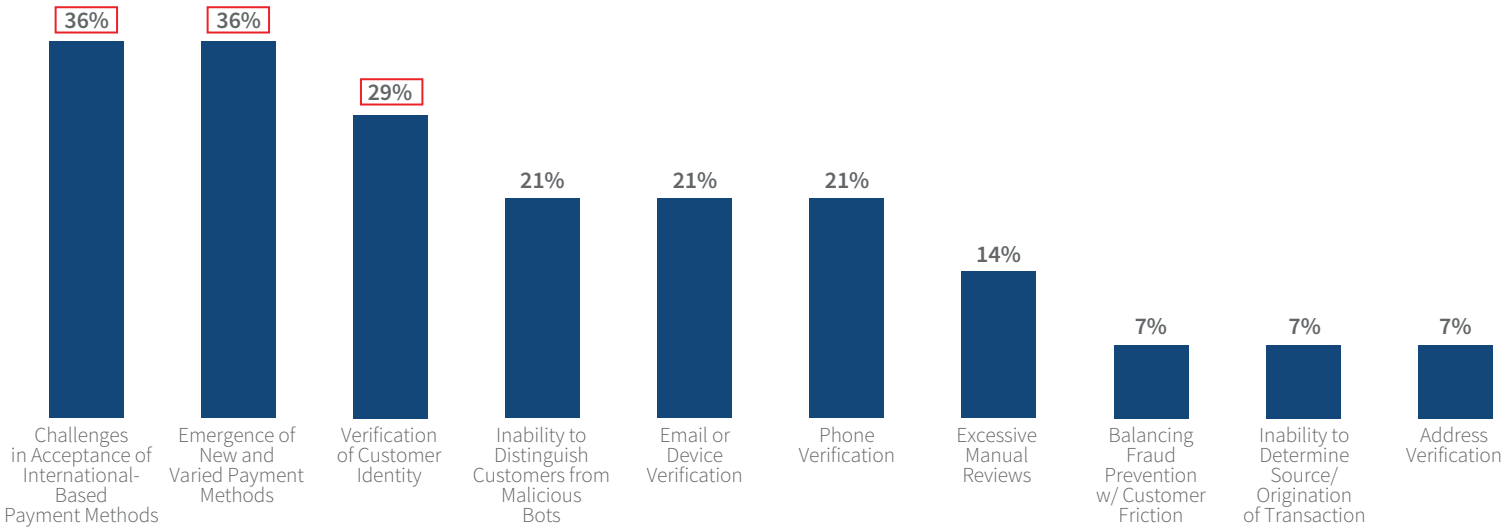
The risk of synthetic identities and malicious bot attacks are top underlying reasons that identity verification is a challenge. There is a need for more real-time 3rd party data, particularly for those who are concerned about balancing fraud detection/prevention with minimizing customer friction.

Botnet attacks and synthetic identity fraud are expected to be among a number of challenges facing merchants and financial institutions over the next 24 months, including where these enable account takeovers.

KEY FINDING 03
FRAUD CHALLENGES

Payment methods, new and non-domestics ones, and identity verification are the top three challenges for Indian merchants that sell digital goods.

Challenges When Selling Digital Goods*
(ranked in top 3)



☐ = significantly or directionally higher than most or all other challenges

Survey Questions:
Q19a_1: Please rank the top 3 challenges related to fraud faced by your company when selling customers digital goods.
Q19a_2: Please rank the top 3 factors that make customer identity verification a challenge when selling digital goods

Top Factors Making ID Verification Challenging

- Limited ability to confirm order location (80%)
- Balancing speed of detection with customer friction (60%)

* Asked only of retail and E-commerce merchants

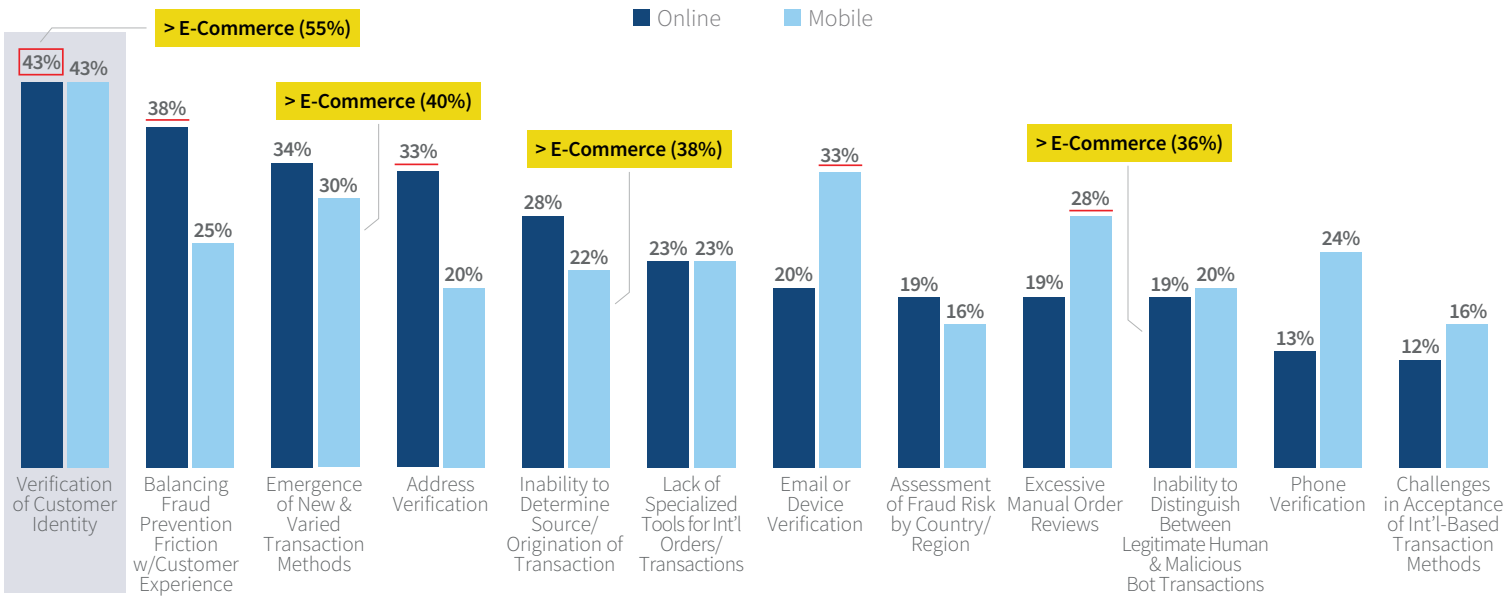
KEY FINDING 03
FRAUD CHALLENGES

Identity verification is a top online and mobile channel challenge for Indian merchants and financial institutions. But there are many other challenges as well.

Various factors contribute to identity verification challenges, including synthetic identities, determining order location and need for real-time data/tools for quickly assess fraud risk while minimizing customer friction.

There are also challenges, in varying degrees, with new payment methods and determining transaction source. Mobile channel challenges include these issues, as well as digital identity verification (e-mail, device, phone), which likely relates to excessive manual reviews.

Fraud Challenges by Transaction Channel
(ranked in top 3)



— = significantly or directionally higher than same challenge in the other channel
□ = significantly or directionally higher than most or all other challenges within channel

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

Top Factors Making ID Verification Challenging

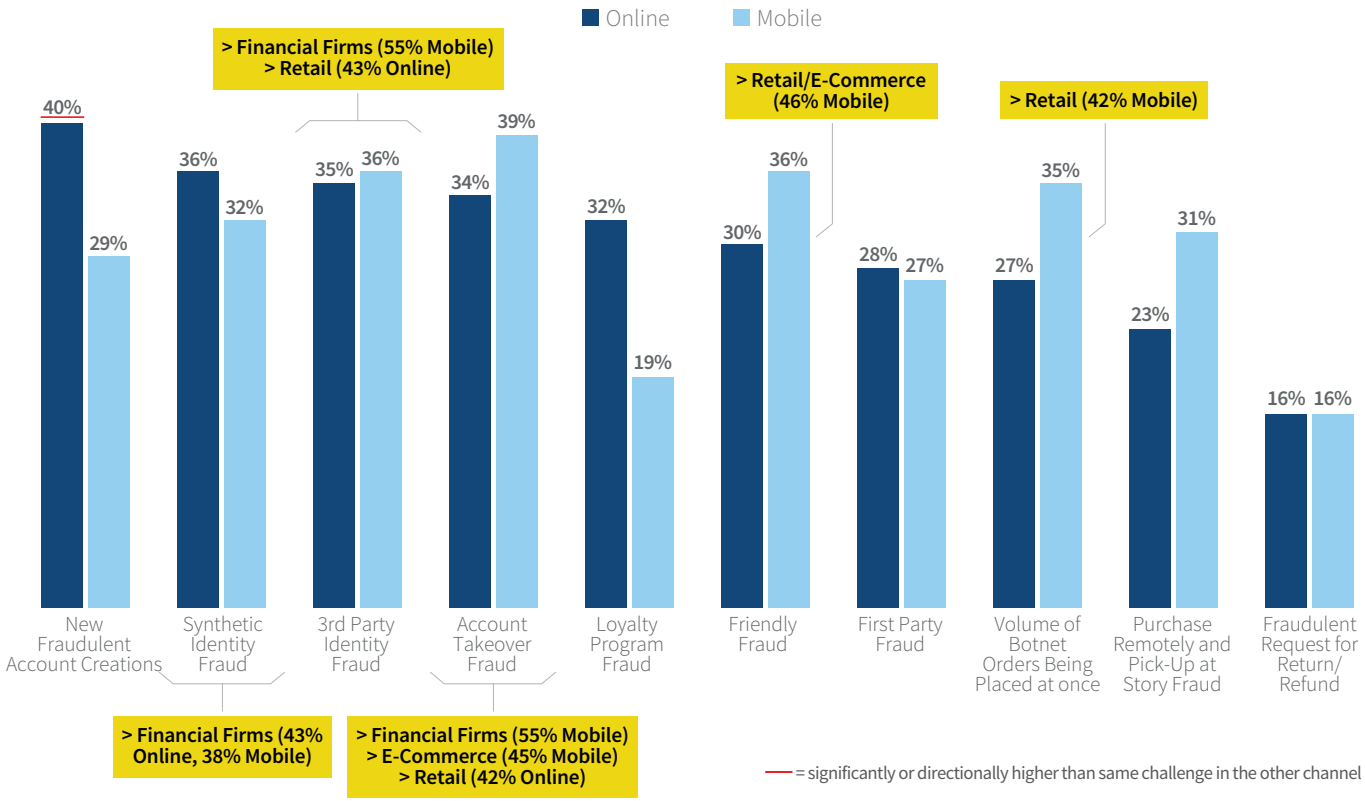
- Rise if synthetic identities (Online 50%; Mobile 60%)
- Volume of malicious bot attacks (Mobile 57%)
- Limited access to real-time 3rd party data (Online 40%; Mobile 44%)

KEY FINDING 03
FRAUD CHALLENGES

Account and identity-related fraud are top online and mobile channel concerns for the next 24 months, in varying degrees across retail, E-commerce and financial institutions.

When looking within specific industry segments, findings show somewhat more concern with mobile channel fraud for the near future. This includes fraud related to identity verification challenges, such as BOPIS (buying online, pick-up at store) fraud, where fraudsters can use fake identities or stolen cards and where store employees are less trained in or don't have access to robust identity verification tools beyond checking one's physical identity attributes (i.e., name, DOB, ID card) that can be forged.

Top Expected Fraud Threats (Next 24 Months)
(ranked in top 3)

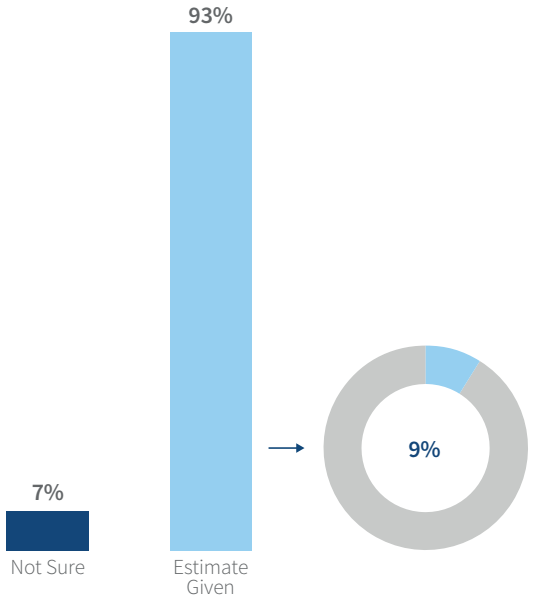


Survey Questions:
Q20e . Please rank the top 3 fraud threats that you expect to face during the next 24 months to fraud when serving customers using the below channel(s).

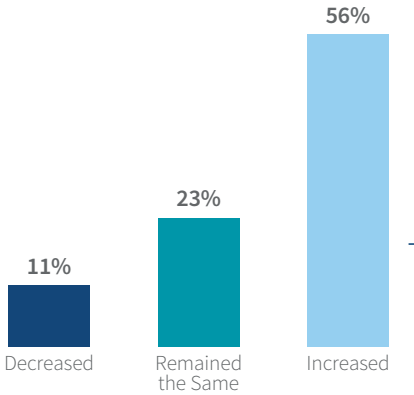
KEY FINDING 03
FRAUD CHALLENGES

Just under one-tenth of Indian merchants' and financial institutions' transactions are estimated as being bots, with just over half of organisations saying that this has increased during the COVID-19 period.

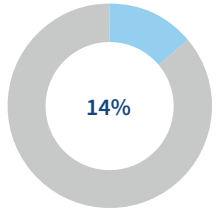
Estimates % of Botnet Activity



% Bot Attacks Compared to Last Year



Average % Increase in Bot Attacks



Survey Questions:
B1a: In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e. rapid creation and placement of hundreds of orders / transactions by fraudulent automated Bots at the same time)?
B1b/c: How does this compare to the same time last year? By how much has the percent of monthly automated malicious bot attacks increased over the past year?

KEY FINDING 04

Merchants and financial services firms that use a multi-layered approach involving passive/digital/transaction risk mitigation solutions that are integrated with their cybersecurity and digital customer experience can more effectively detect and prevent fraud, minimise customer friction and lower their cost of fraud.

Customer friction is a real concern with fraud prevention efforts, especially in the online/mobile channels where abandonment is common with customer effort and transaction delays.

Online/mobile channels are increasingly risky for fraud as new payment and transaction methods provide additional points of entry for sophisticated fraudsters.

Currently, only a few Indian merchants and financial institutions are integrating their cybersecurity and digital customer experience operations with their fraud prevention strategy. This includes a limited number that are extremely focused on minimizing customer friction or using fraud detection solutions that will lessen customer effort.

But, findings show that organisations which use the best-practice of multi-layered solutions designed to minimise friction and assess both physical and digital attributes, along with the above mentioned integration, are less often challenged by identity verification and balancing fraud/friction while also lowering their cost of fraud compared to others.

KEY FINDING 04
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

KEY FINDING 04
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

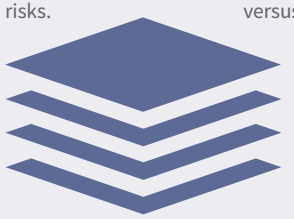
- Cybersecurity Alerts
- Social Media Intelligence
- AI/ML Models
- Crowdsourcing
- Cybersecurity Operations
- Digital / Customer Experience Operations

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 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

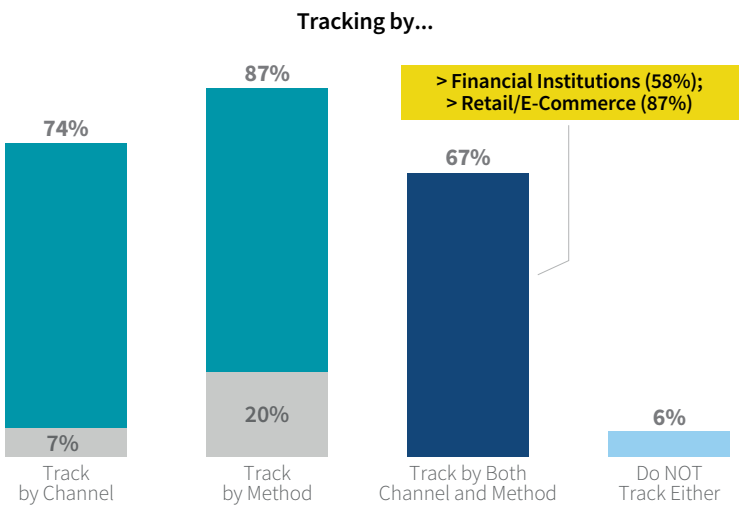
KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

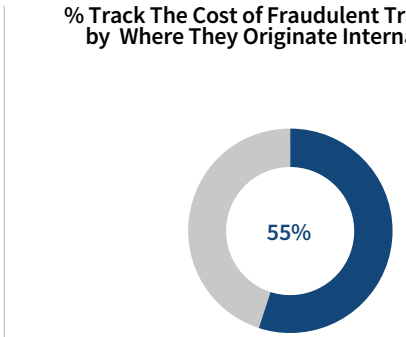
Tracking fraud costs by both transaction channel and payment method is essential to fraud prevention. Two thirds of Indian merchants and financial firms are doing this.

Since fraud occurs in different ways depending on selling physical or digital goods and if using the mobile channel, this creates multiple endpoints and ways that fraudsters can attack. They continue to test for the weakest links and where they can operate undetected. Knowing where fraudsters have been successful is important for "plugging the gaps"; but also knowing where they've tried and failed is important in order to maintain vigilance.

Only half of merchants and financial firms are tracking fraud costs from where they originate, though determining transaction origination / order location is a struggle for most.

% Businesses Tracking Fraud Costs by Channel and/or Payment Method





Survey Questions:
Q14a: Does your company track the cost of fraudulent transactions by payment channels or methods used?
Q14b: Does your company track the cost of fraudulent transactions by where they originate internationally (i.e., coming from specific regions)?

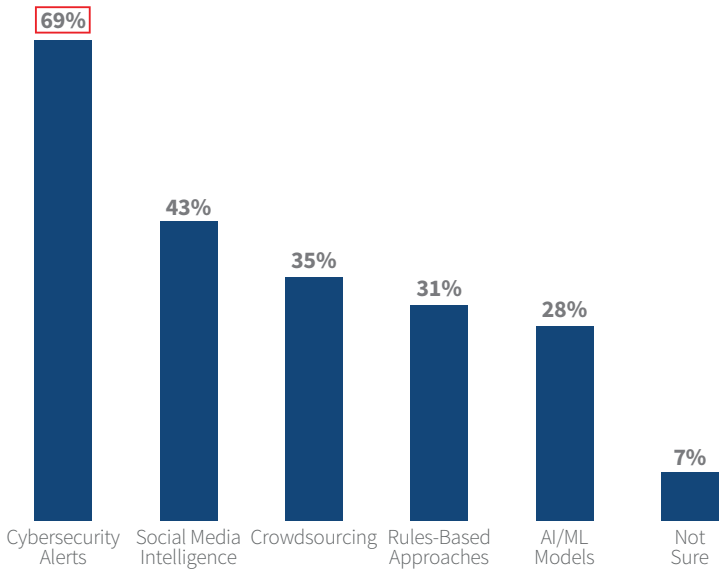
KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

A majority of financial institutions are using Cybersecurity Alerts to support fraud prevention. There is some use of Social Media intelligence, but less so with AI/ML. Integrating fraud approaches with cybersecurity operations and the digital customer experience is also limited.

% Using Best-in-Class Fraud Mitigation Practices

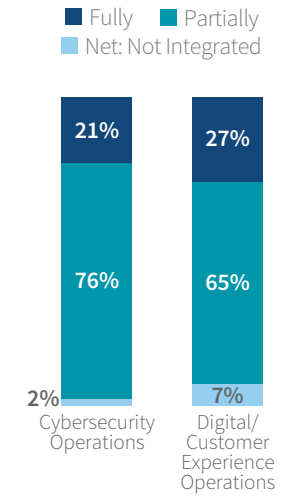
% Using Supportive Capabilities to Fight Fraud

Financial firms are more likely to use Cybersecurity Alerts (83%) and Crowdsourcing (48%)



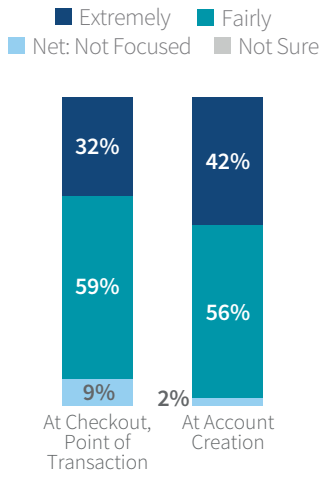
☐ = significantly or directionally higher than most or all other challenges within channel

Integration of Cybersecurity & Digital/Customer Experience Operations w/Fraud Prevention



Retail is farther ahead with being fully integrated with cybersecurity (35%) and the digital experience (39%), though this still represents a minority of organisations across sectors

Degree Focused on Minimizing Customer Friction Through Online/Mobile Channels



43% of financial firms are extremely focused on minimizing online/mobile friction at point of transaction; 47% are focused on this at account creation

Survey Questions:
Q28b: In addition to solutions, what supportive capabilities is your company using to help fight fraud?
Q29. To what degree has your company integrated its cybersecurity operations with its fraud prevention efforts?
Q30. To what degree is your company focused on minimizing customer friction through online/ mobile channels
Q30b. To what degree has your company integrated its digital/ customer experience operations with its fraud prevention efforts?

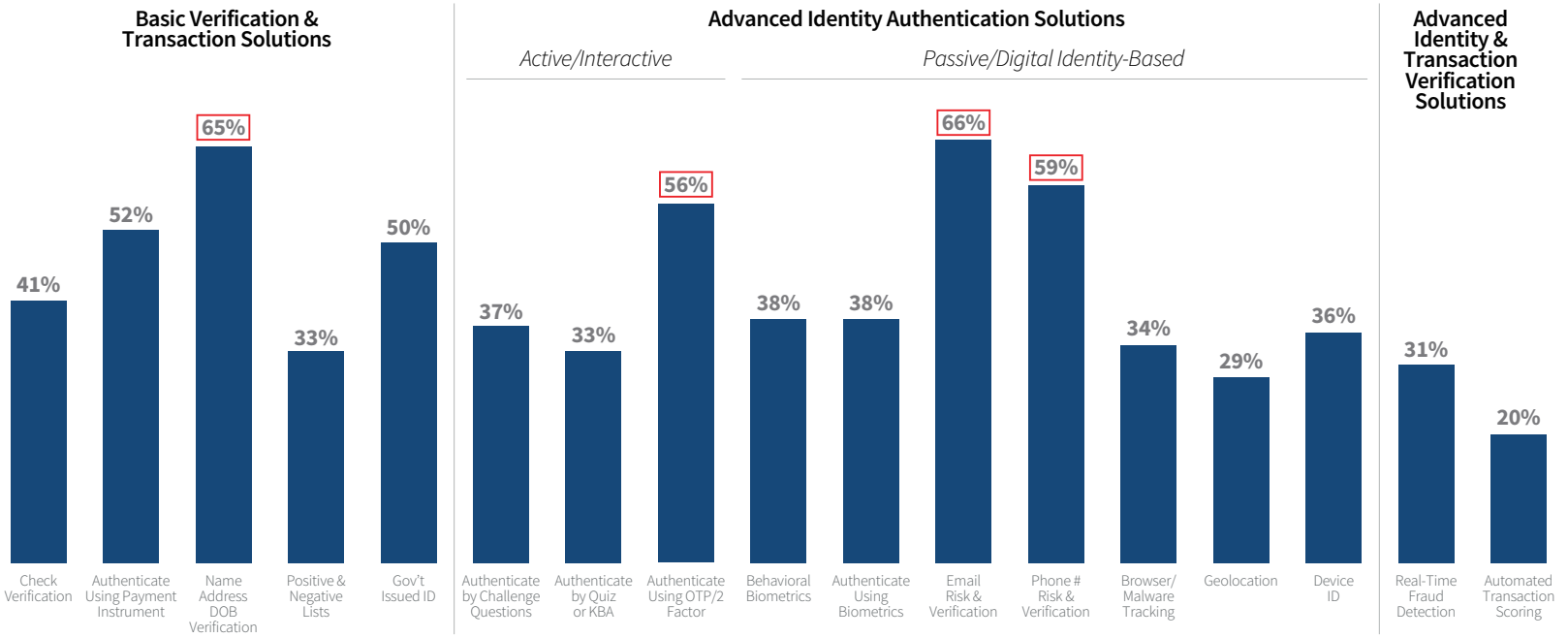
KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

While e-mail/phone risk verification and OTP authentication are reportedly used by a majority of Indian merchants and financial institutions, there is limited use of digital identity-based and transaction-risk assessment solutions.

A best-practice is to assess both the physical (name, DOB, address) and digital (device, e-mail, phone number, browser) attributes of an identity, as well as the risk of the transaction as well, particularly in real-time. This addresses the various points of entry by fraudsters, a more holistic understanding of the identity and its behaviours in order to distinguish anomalies and do so in a way that minimises customer friction.

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

Fraud Mitigation Solutions Usage



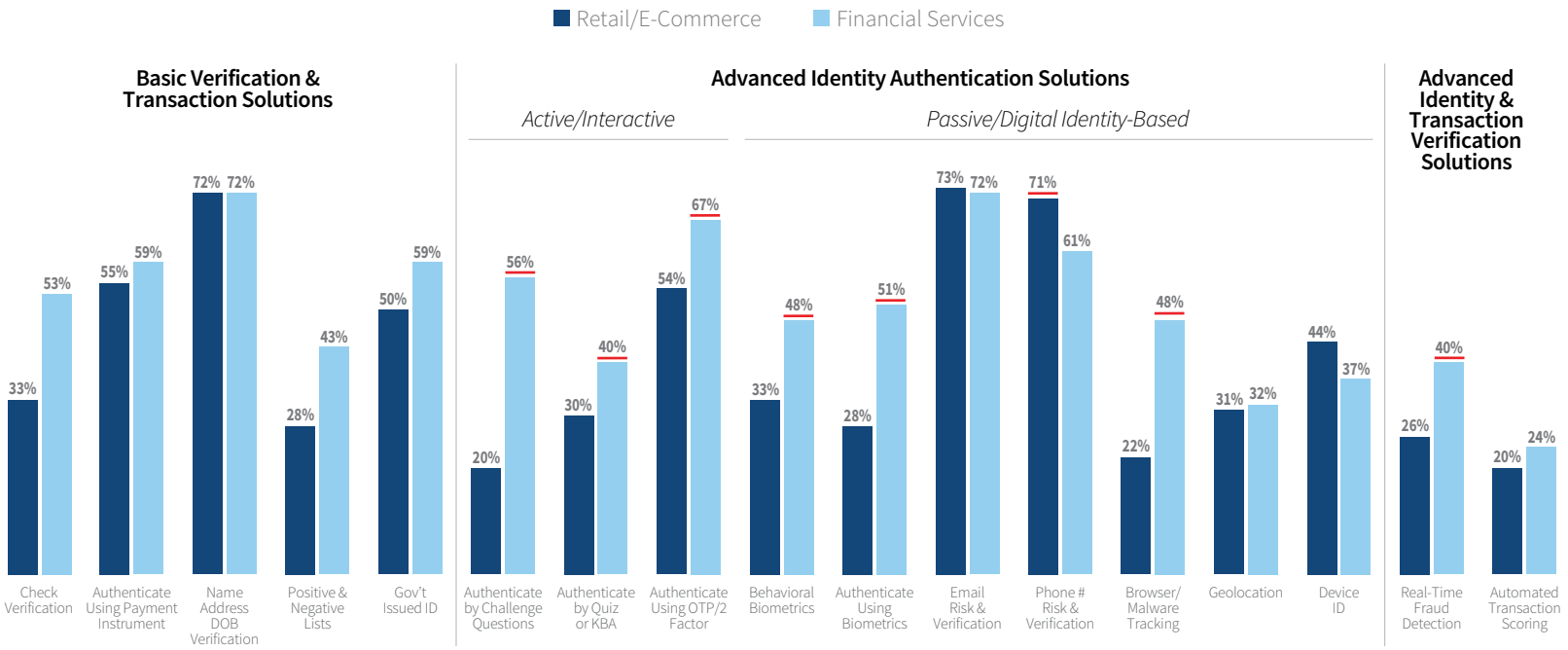
☐ = significantly or directionally higher than most or all other challenges within channel

KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

To the degree there are differences in solutions use by industry, Indian financial institutions are more likely to use additional advanced identity authentication solutions.

These address the various points of entry by fraudsters, and provide a more holistic understanding of the identity and its behaviours in order to distinguish anomalies and do so in a way that minimises customer friction.

Fraud Mitigation Solutions Usage:



= significantly or directionally higher than same solution in the other segment

Survey Questions:
Q27: Which of the following fraud solutions does your company currently use at the point of purchase /distribution of funds?

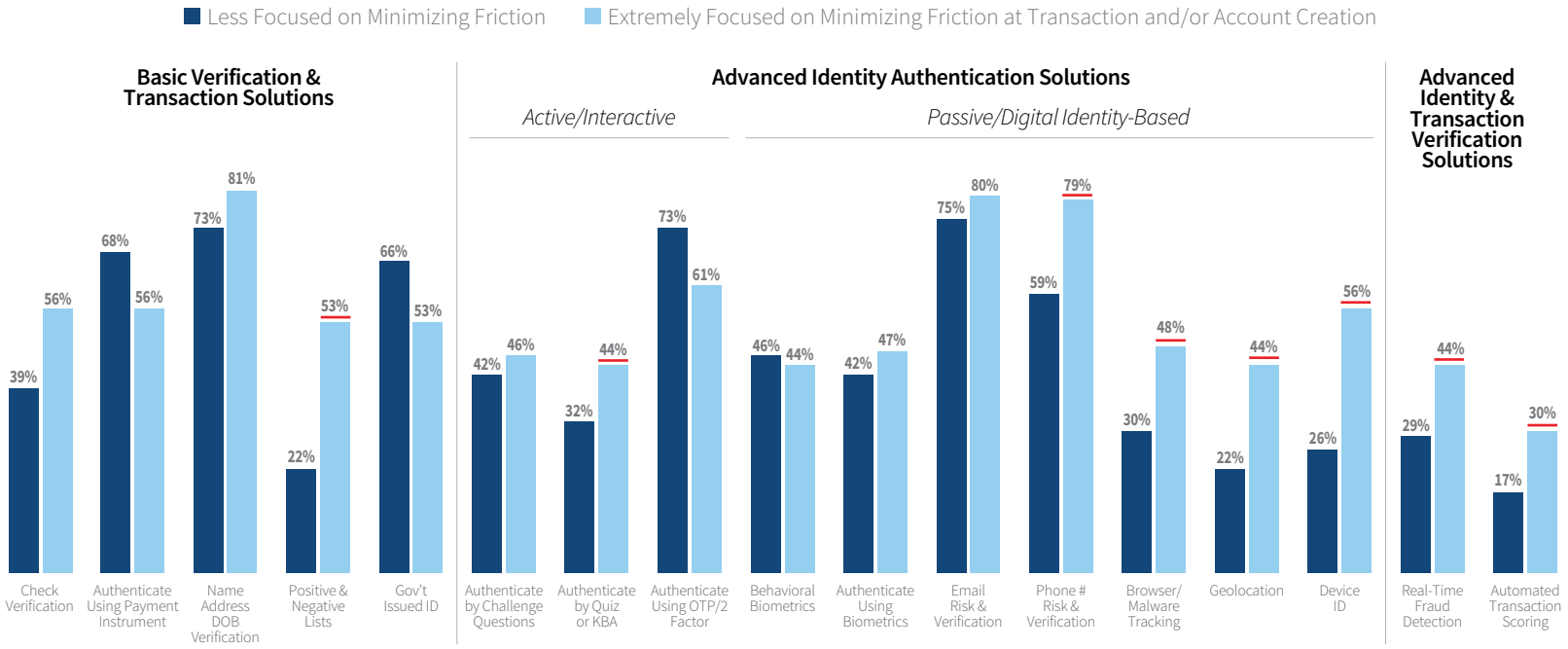
KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

Indian merchants and financial institutions that focus on minimizing customer friction are more likely to use passive/digital identity and transaction verification solutions than others.

These provide fast, seamless, and "behind the scenes" fraud detection that reduces customer efforts and delays. And many of these organisations say that they've done extremely well in managing fraud detection with friction.

Fraud Mitigation Solutions Usage:

Comparison by Degree of Focus on Minimizing Customer Friction



Survey Questions:
Q27: Which of the following fraud solutions does your company currently use at the point of purchase /distribution of funds?

— = significantly or directionally higher than same solution in the other segment

Those extremely focused on minimizing friction at point of transaction are significantly more likely to feel that they have managed fraud detection & friction at this stage than others (45% vs. 8%)

KEY FINDING 04
FRAUD DETECTION & PREVENTION APPROACHES

The cost of fraud, customer friction and its challenges are lessened for organisations that invest in a multi-layered risk mitigation solutions that focuses on minimising customer friction and is integrated with cybersecurity and digital customer experience operations.

While investing in solutions that assess digital identity attributes and transaction risks, organisations are also reducing the burden on legitimate customer effort (letting customers in) while more effectively detecting and blocking fraudsters. As a result, they experience significantly fewer challenges with identity authentication and balancing fraud prevention with customer friction while also lowering their cost of fraud.

REGIONAL LEVEL DATA

	Best Practice Multi-Layered Solution Approach*	Those NOT following Best Practice Multi-Layered Solution Approach
Solution(s) to **verify physical attributes** (e.g., Name, Data of Birth, Address)		
Solution(s) to **verify digital attributes** (e.g., E-mail, phone number risk, biometrics)		Limited or None
Solution(s) to **assess device risk, location** (e.g., Device ID, Geolocation)		Limited or None
Solution(s) to **assess behaviour** (e.g., Behavioural Biometrics, Transaction Risk)		Limited or None
	Plus Fraud Ops integrated with Cybersecurity/Digital Experience and Extremely focused on minimizing customer friction	**Not integrated and focused on minimizing customer friction**
	Online Mobile	**Online Mobile**
% Ranking identity verification as a top online/ mobile challenge	**25% / 37%**	**57% / 42%**
% Ranking balancing fraud prevention with friction as top online/mobile challenge	**18% / 14%**	**47% / 28%**
For every fraudulent transaction, the cost is . . .	**3.45 times lost value**	**4.00 times lost value**

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

RECOMMENDATION #1

Technology Innovation 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 to enable 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

Multi-Layered Fraud Defense is Required

- Single point protection is no longer enough for effective fraud prevention.
- User behaviors including transaction patterns, payment amounts, and payment beneficiaries, are becoming more varied and less predictable with customers transacting cross locations and geographies.
- 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.
- It is important that the fraud defense platform is able to examine malware level threats, Bot, remote access Trojan and IP spoofing detection across web and mobile channels as well as provide behavioral analytics to help reduce false positives.

RECOMMENDATION #3

Identity Fraud with something simple – Email addresses

- Email addresses are ideally suited to identify customers as part of your organization's fraud and identity management strategy. After all, email is already a primary contact channel that organizations use to reach their customers.
- Additional layer of security can begin with verifying a consumer's identity and assessing risk at multiple customer touchpoints like account opening, account maintenance and online transactions.
- Enhanced security can be achieved by evaluating email address metadata points such as domain details, email details, risk indicators and, when available, other personally identifiable information (PII) to assess the risk level. The associate decisioning data and a risk score can help stop fraud without negative impact to genuine customers, in a simple and efficient manner.

RECOMMENDATION #4

Tactics against BOT attacks - Behavioral Biometrics

- Organization can add additional layer of defense by analyzing the way a user interacts with a device and reliably differentiates between different user profiles.
- It will provide additional risk signals across account openings, high-risk pages and payments and create a unique profile for users by analyzing patterns in their activities
- It helps to distinguish between human, bot account activities and detect session anomalies and at the same time, confidence relating to returning, trusted customers

RECOMMENDATION #5

Cybersecurity and digital customer experience operations must be integrated with your fraud processes

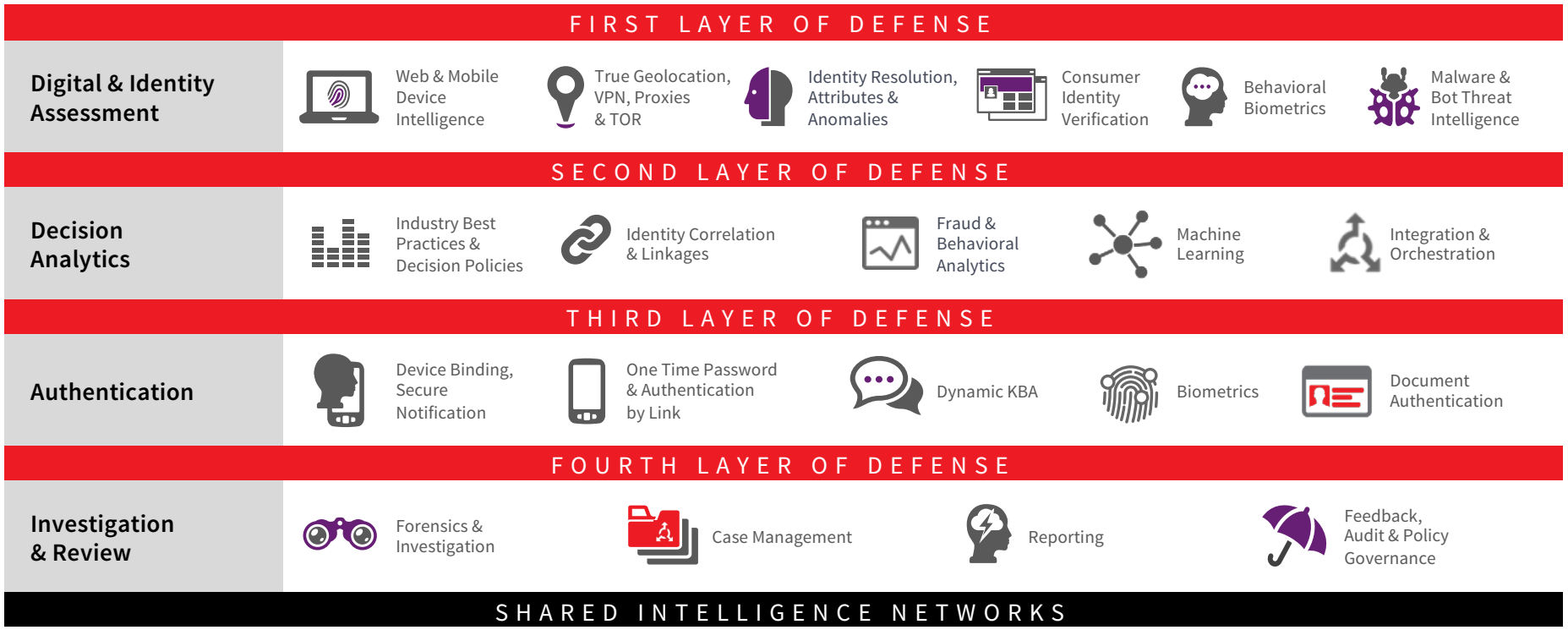
- Improve decisions and the customer experience with machine learning and an integration of systems/resources that manage risk across the business and all endpoints – risk convergence.
- Enhanced data and analytic capabilities from tools such as AI/ML, cyber alerts, Social Media intelligence and Crowdsourcing lets businesses predict threats rather than react to them.
- Integrating these tools with digital identity-based solutions provides protection across the customer journey, not just at the point of transaction; most fraudsters prefer account-related takeovers / creation because this provides an ongoing source of assets instead of a one-time transaction.
- Combined, the above can provide efficiencies and cost savings, as well as ensuring an optimised customer experience, particularly where fraud risks can be segmented so that security controls can be adjusted upwards or downwards based on the transaction.

RECOMMENDATION #6

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

Our Fraud Portfolio Enables a Multi-Layered Identity Verification and Authentication Strategy For Digital And Physical Identity Intelligence



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 for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

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