Research Definitions

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

The research provides a snapshot of:

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

Fraud Definitions

Fraud is defined as the following:

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

This research covers consumer-facing fraud methods

» It does not include insider fraud or employee fraud

The LexisNexis Fraud Multiplier℠

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

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

<table>
<thead>
<tr>
<th>Surveyed Industries</th>
<th>Singapore</th>
<th>Indonesia</th>
<th>Malaysia</th>
<th>Philippines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>e-Commerce</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Financial Services</td>
<td>30</td>
<td>30</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>90</strong></td>
<td><strong>90</strong></td>
<td><strong>90</strong></td>
<td><strong>90</strong></td>
</tr>
</tbody>
</table>

Surveyed industries include:

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

- **e-Commerce**
  - Earn 80% or more of revenues through online channels

- **Financial Services**
  - Retail/Commercial Banks
  - Credit Unions
  - Investments
  - Trusts
  - Wealth Management

*Use of the phrase "surveyed industries" throughout the report refers to Retail, e-Commerce, and Financial Services
### Segment Definitions

#### Online Channels

- **Web Browser**
  Transactions through a computer/web browser

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

- **m-Commerce**
  Transactions specifically through mobile browser and/or mobile apps

#### Digital

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

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

**Digital Financial Services**
Earn 50% or more of revenues through online channels
Key Findings

1. The cost of fraud for surveyed industries in Malaysia is 3.57 times the lost transaction value. 
   - This appears to be driven higher by Financial Services businesses, where the cost of fraud is 3.96 times the value of the lost transaction.

2. The mobile channel is contributing to fraud risk among surveyed industries in Malaysia. 
   - This includes both mobile web browsers and mobile apps.

3. Customer identity verification is a key issue for online channels. 
   - Limited/no tracking tools and botnet attacks are contributing factors for mobile. Limited ability to confirm order location and synthetic identities are key for web browser.

4. Businesses in surveyed industries that offer m-Commerce suffer from the cost of fraud. But Digital Financial Services firms (regionally) suffer even more. 
   - For every fraudulent incident, the cost to businesses that offer m-Commerce is actually 3.95 times the amount of the lost transaction value, totaling fraud costs that are 2.05% of annual revenues. And this cost is even higher, up to 4.09 times the lost transaction amount, for Digital Financial Services firms across study countries.

5. Businesses across surveyed industries are not fighting fraud in an effective way. 
   - 43% reportedly do not track successful fraud transactions by both channel and payment method. Additionally, an average of 60% of flagged transactions continue to be sent for costly and time-consuming manual reviews.

6. The use of more advanced fraud mitigation solutions is limited. 
   - The use of more advanced solutions, and those geared toward mobile fraud detection, such as Digital Identity, Geolocation, and OTP/2 factor is limited.
The cost of fraud for surveyed industries in Malaysia is 3.57 times the lost transaction value.
The LexisNexis Fraud Multiplier℠ is 3.57 across surveyed industries.

» This means that for every fraudulent transaction, the cost to Malaysian businesses is actually 3.57 times the amount of the lost transaction value. This translates to fraud costs amounting to 1.93% of annual revenues overall.

» Country-level fraud volumes and costs appear to be driven up, in part, by the Financial Services sector, where volumes and costs are higher. And whilst anecdotal (given small base sizes), the cost of fraud for Financial Services is directionally higher in Malaysia (3.96 times the face value of the lost transaction) than in the United States (2.92 times). Some of this could relate to a 78% year-on-year growth in Financial Services attack rates for new account creations in the region.

» The mobile channel, digital goods sales, and limited use of solutions to address specific threats are part of the reason for higher risks and costs.
**How is the LexisNexis Fraud Multiplier℠ calculated?**

**LexisNexis Fraud Multiplier℠**

![Diagram](https://via.placeholder.com/150)

**Illustration**

Calculating the LexisNexis Fraud Multiplier℠

**Description**

The total cost for every RM 1 of fraud, calculated as total losses divided by the amount of fraudulent transactions for which the firm is held liable.

**Step 1:** Obtain average revenue RM 6,977,154,203*

**Step 2:** Obtain fraud as % of annual revenue from Q10 1.93%

**Step 3:** Calculate total cost of fraud (Steps #1 x #2) RM 134,659,076

**Step 4:** Obtain % of total losses for lost transaction values (actual values of the fraudulent transactions that occurred) (Q16) 28.05%

**Step 5:** Calculate actual value of the fraudulent transaction that occurred (Steps #3 x #4) RM 37,771,871

**Step 6:** Calculate total cost for every S$ 1 of fraud (total cost in Step 3) / (value of fraudulent transactions in Step 5) $3.57

---

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

Market Conditions

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

» Ranks 5th among the fastest growing e-Commerce countries in 2019, above the global average.2

» 121% growth in transactions performed via mobile devices from 2017 to 2018.3

» Barriers to secure payment methods; sizeable unbanked population that requires merchants to attract these consumers through alternative payment methods and mobile devices which may not always be secure.

Cybercrime threats:

» One of the top reported crimes last year was identity theft (using IC number, birth date, bank account number), accounting for over 40% of reported cyber crimes. The personal data used in this identity theft was likely obtained from the many data breaches over the past years, as only 4% of the data was encrypted.4

» Cyber crimes involving losses of RM67.6 million in over 2,000 cases were reported in the first three months 2019.5

Transaction Risks

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

Risks from mobile browser and mobile app transaction methods.

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

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

---

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

» Where non-Malaysia fraud occurs, a majority comes from other Southeastern Asian markets.

» There is a disproportionate degree of fraud other regions as compared to their revenue contributions. This follows a growing trend with attack dispersion, in which attackers are beginning to target markets outside of their region.6

6 ThreatMetrix® H2 2018 Cybercrime Report
The mobile channel is contributing to fraud risk among surveyed industries in Malaysia.
A majority of transactions go through the in-person and online channels.

- Though mobile channel transaction volumes are modest compared to other types, m-Commerce is growing rapidly in Malaysia. The increase of mobile network operators, the ubiquity of commercial banks offering m-Commerce services, and the increase in market size, all demonstrate that the m-Commerce sector is growing. In fact, 62% of mobile users use their devices to shop online.7

- Among businesses offering m-Commerce, the greatest portion of transactions occur through branded and 3rd party mobile apps, followed by mobile web browsers.

- Whilst mobile web browsers have historically been considered less secure, fraudsters are now increasingly targeting mobile apps at a global level8, driven in part by click flooding and botnet attacks. Shopping, gaming, and financial apps are hit the hardest. Botnets attack devices through malware and can then imitate legitimate transactions coming from a mobile app. Device owners may not even be aware of this.

---

7 https://www.export.gov/article?id=Malaysia-E-Commerce
8 https://www.appsflyer.com/resources/the-state-of-mobile-fraud-q1-2018/
However, mobile transaction risk seems to be an accepted trade-off for providing customer convenience and to grow business.

Reasons For Accepting Mobile Transactions
(among those transacting through the mobile channel)
Traditional payment methods are largely accepted (credit, cash, debit cards), but mobile apps are accepted just as much, as businesses seek to include unbanked customers.

» In Malaysia, the population of the unbanked is reported to be at ~8%, or two million of the country’s 24 million adults. Whilst this may seem small in comparison to neighbors, such as Indonesia and the Philippines, whose unbanked make up more than half the population, there is still a need to capture this segment in order for Malaysia to become a cashless society.  

» In fact, the United Nations Capital Development Fund (UNCDF), Bank Negara Malaysia (BNM), and Malaysia Digital Economy Corporation (MDEC) launched the Digital Finance Innovation Hub to further support the financial inclusion of Malaysia’s middle and low-income people.  

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

- Debit Transaction: 98%
- Credit Transaction: 98%
- Cash: 93%
- Mobile Wallet Apps (3rd Party & Branded): 93%
- Gift Cards: 13%
- Virtual Currency: 9%
- 3rd Party Payment Providers Such as PayPal, etc: 7%
- Other Alternative Transaction Methods Such as BillMeLater, eCheque: 3%
- Social Media Payments: 1%

Ways to Reach Unbanked Consumers

9 https://www.theedgemarkets.com/article/integrating-unbanked-cashless-society  
Customer identity verification is a key issue for online channels.
Customer identity verification is a key challenge for online channels.

» This isn't surprising, given that identity theft is one of the top reported cybercrimes in the country.

» Other challenges are varied.

### Top 3 Challenges Related to Fraud When Serving Customers Through...

(among those transacting through each channel)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Web Browser</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of Customer Identity</td>
<td>36%</td>
<td>57%</td>
</tr>
<tr>
<td>Inability to Determine Source/Origin of Transaction</td>
<td>30%</td>
<td>28%</td>
</tr>
<tr>
<td>Phone Verification</td>
<td>27%</td>
<td>26%</td>
</tr>
<tr>
<td>Inability to Distinguish Between Legitimate Human &amp; Rot Transactions</td>
<td>37%</td>
<td>23%</td>
</tr>
<tr>
<td>Balancing Fraud Prevention Friction w/Customer Experience</td>
<td>27%</td>
<td>20%</td>
</tr>
<tr>
<td>Challenges in Acceptance of Int'l-Based Transaction Methods</td>
<td>23%</td>
<td>20%</td>
</tr>
<tr>
<td>Emergence of New &amp; Varied Transaction Methods</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>Email or Device Verification</td>
<td>21%</td>
<td>16%</td>
</tr>
<tr>
<td>Address Verification</td>
<td>12%</td>
<td>15%</td>
</tr>
<tr>
<td>Excessive Manual Order Reviews</td>
<td>11%</td>
<td>9%</td>
</tr>
<tr>
<td>Assessment of Fraud Risk by Country/Region</td>
<td>10%</td>
<td>8%</td>
</tr>
</tbody>
</table>

68% Through Online Channels

57% 57%
Key factors that challenge customer identity verification differ somewhat by channel.

» Limited/no tracking tools and volume of malicious botnet orders contribute to difficulties through mobile. Limited ability to confirm order location and the rise of synthetic identities are key inhibitors for web browser.

» As prevention technologies have improved to stop activities such as card skimming, criminals are now stealing identities or constructing “fake” people. The availability of personal information online via social media platforms and mobile apps has made it easier for culprits to mix fake and real personal information. 6 in 10 APAC banks reportedly experienced synthetic identity fraud in 2018.\(^\text{11}\)

---

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

<table>
<thead>
<tr>
<th>Factor</th>
<th>Web Browser</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited/No Real-Time Transaction Tracking Tools</td>
<td>65%</td>
<td>36%</td>
</tr>
<tr>
<td>Volume of Malicious Botnet Orders Being Placed at Once</td>
<td>52%</td>
<td>23%</td>
</tr>
<tr>
<td>Limited Ability to Confirm Order Location</td>
<td>57%</td>
<td>39%</td>
</tr>
<tr>
<td>Rise of Synthetic Identities</td>
<td>48%</td>
<td>42%</td>
</tr>
<tr>
<td>Limited/No Access to Real-Time Third Party Data Sources</td>
<td>34%</td>
<td>28%</td>
</tr>
<tr>
<td>Balancing Speed of Approval Against Customer Friction</td>
<td>42%</td>
<td>39%</td>
</tr>
</tbody>
</table>

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

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

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

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

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

### Risks & Challenges

- **Extremely Hard to Distinguish from Legitimate Customers**
  - Focus on nurturing the identity to mimic a good customer, establishes good credit, pays on-time, etc. before "breaking bad"

- **Difficult to detect with traditional identity verification / authentication solutions**
  - These are professional fraudsters; they often know the types of information required to gain approval and pass certain checkpoints. Use of real identity data helps them do this.

- **Real customers don’t help; behaviours make it difficult to spot anomalies with current ID solutions.**
  - Consumers have more ways to purchase, from different locations anywhere and anytime. They might share passwords and use different devices at different times. It is harder to make physical and digital connections that distinguish fraudulent from legitimate patterns.
Many across surveyed industries believe that reducing fraud can help to drive revenues and customer loyalty.

» However, this is complicated by doubts regarding the mobile channel/payment types and digital goods.

» This underscores the importance of putting effective fraud mitigation solutions in place.

**Perception of Fraud (% agree)**

- Reducing fraud can help increase my company’s revenues: 68%
- Security of mobile device transactions still unknown: 58%
- Lower fraud rates increase customer loyalty: 57%
- Selling digital goods increases the risk of fraud: 57%
- Evolution of mobile payment & channel adds significant risk of fraud: 56%
- Fraud is inevitable: 55%
- e-Gift card fraud will continue to rise in the future: 52%
- Combating automated Botnet activity is overwhelming: 49%
- Increasingly difficult to manage fraud prevention whilst minimizing customer friction: 45%
- Costs too much to control fraud: 42%
- Transacting via mobile channel is more secure than the web browser: 33%

*Asked only of Retail/e-Commerce selling digital goods*
Businesses in surveyed industries that offer m-Commerce suffer from the cost of fraud. But Digital Financial Services firms (regionally) suffer even more.
A large share of fraud, approximately 63%, occurs through online channels.

» Mobile transactions in the region are experiencing a growth in attack rate of 17% year-on-year.¹²

» Whilst mobile web browsers account for the single largest amount of fraud losses, branded and 3rd party mobile apps account for more, combined. This shows that fraudsters are targeting them, often through click flooding and botnet attacks.

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

63% through online channels

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

*% can add to more than 100% since answers based on using a channel
12 ThreatMetrix® H2 2018 Cybercrime Report
Approximately 31% of fraud losses can be attributed to identity fraud (3rd party identity theft/synthetic identity).

- Fraud from account takeovers and fraudulent account creations represents significantly more identity-based fraud than that coming from purchases or transactions.

- New e-Commerce account creation transactions from Southeast Asia are attacked at a very high rate of 41%. And new account creations attacks in the Financial Services sector have grown by 78% overall, and 105% through mobile devices.  

13 Ibid.
Whilst credit and debit transactions account for most of fraud losses, alternative and other methods (that include web and mobile options) losses are sizeable.

- Stolen cards and CNP make up the majority of fraud losses.

- A study done by Bank Negara Malaysia showed that most credit card losses were incurred when the card wasn’t even present, with either stolen PIN numbers or CVV codes.

- In response to such fraud, RHB is introducing fraud protection cards with mini screens on the back that auto-generate new card verification value (CVV) numbers. An algorithm will generate the new number for the card. It offers an alternative to standard cards with a static CVV code that only changes when the card is replaced.14

*% can add to more than 100% since answers based on whether using a channel

65% of businesses across surveyed industries have experienced an increase in automated botnet activity over the past year.

» This is a growth of 16% of transactions on average.

<table>
<thead>
<tr>
<th>Botnet Activity as % of Transactions Per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Sure</td>
</tr>
<tr>
<td>2%</td>
</tr>
<tr>
<td>6%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change in Volume of Botnet Activity Over Past Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decreased</td>
</tr>
<tr>
<td>9%</td>
</tr>
<tr>
<td>16%</td>
</tr>
</tbody>
</table>
The combination of these factors contribute to increased risk.

<table>
<thead>
<tr>
<th>Mobile</th>
<th>Cross Border</th>
<th>Digital</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Rise of mobile botnet attacks; malware infects devices without</td>
<td>» Uncertainties, blind spots and new payment methods; it becomes difficult</td>
<td>» Fast transaction; digital goods/services, such as downloads and</td>
</tr>
<tr>
<td>consumer knowledge; steals identity, hacks accounts, makes fraudulent</td>
<td>to determine transaction origination; lack of verifiable data on consumers</td>
<td>subscriptions, tend to occur quickly; lack of a physical delivery</td>
</tr>
<tr>
<td>purchases(^{15})</td>
<td>(particularly with GDPR)</td>
<td>address eliminates buffer period for fraud verification before shipment;</td>
</tr>
<tr>
<td>» Consumer risk behaviours – using open WiFi networks increases risk</td>
<td></td>
<td>with fear of abandonment, merchants struggle with balancing fraud</td>
</tr>
<tr>
<td>of smishing (SMS-based phishing) and man-in-the-middle interception</td>
<td></td>
<td>prevention and minimising customer friction.</td>
</tr>
<tr>
<td>of passcodes used for multi-factor authentication(^{16}); “keep me</td>
<td></td>
<td>» Favourite target for fraudster card testing; use of bots to test stolen</td>
</tr>
<tr>
<td>logged in” habits become an unlocked entry point to accounts</td>
<td></td>
<td>credit card information with lower value goods/services (typical of</td>
</tr>
<tr>
<td>» Increasing pool for fraudster opportunity as more people conduct</td>
<td></td>
<td>digital goods/services) tend to arouse less suspicion.</td>
</tr>
<tr>
<td>mobile transactions</td>
<td></td>
<td>» Easy targets; synthetic identities and stolen data make it difficult</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to distinguish between malicious attacks and legitimate customers in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>anonymous channel.</td>
</tr>
</tbody>
</table>

\(^{15}\) Ibid.  
This results in higher volumes and cost of fraud for businesses that offer m-Commerce.

» Every fraudulent transaction actually costs these businesses 3.98 times the value of lost transaction. This is higher than the average across organisations (3.57) overall.

» This channel also experiences a higher number of successful fraud transactions that involve higher average values.

Among Businesses Offering m-Commerce

<table>
<thead>
<tr>
<th>LexisNexis Fraud Multiplier™</th>
<th>Fraud as % Cost of Revenues</th>
<th>Average # Reported Successful Fraud Transactions per Month*</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.95</td>
<td>2.05%</td>
<td>596 Retailers/e-Commerce 2,560 RM Financial Services</td>
</tr>
</tbody>
</table>

x face value of lost transaction

* Based on self-reported numbers and likely recall; not meant to be exact; may increase or decrease based on seasonality
Regionally, those that are “digital” have even higher risks and costs associated with fraud, which tends to overlap with m-Commerce.

» For digital Retailers, e-Commerce merchants, and Financial Services businesses, identity verification becomes a challenge and a risk.

» For Retailers/e-Commerce merchants, speed and type of transaction are the issue. Digital goods/services involve more immediacy of distribution/downloading; whereas merchants that sell physical goods have a delivery address for shipping and a buffer time between transaction and shipment to confirm identity and legitimacy of the sale, this is not the case for those selling digital goods. There is more real-time need for fraud detection efforts.

» For Financial Services businesses, the anonymity of the online channels makes identity verification much more difficult.

» And, with all segments, devices (computers, tablets, mobile phones) can confuse things with spoofing and malware.

» Across industries, those that are digital get hit with a higher cost of fraud.

LexisNexis Fraud Multiplier<sup>SM</sup>

<table>
<thead>
<tr>
<th>Retailers/e-Commerce Merchants (Regional Level Across APAC Study Countries)</th>
<th>Financial Services Businesses (Regional Level Across APAC Study Countries)</th>
</tr>
</thead>
<tbody>
<tr>
<td>times face value of lost transaction</td>
<td>times face value of lost transaction</td>
</tr>
<tr>
<td>Does NOT Sell Digital Goods/Services</td>
<td>2.71</td>
</tr>
<tr>
<td>DOES Sell Digital Goods/Services*</td>
<td>3.09</td>
</tr>
<tr>
<td>3.88</td>
<td>4.09</td>
</tr>
</tbody>
</table>

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

** earn 50% or more of revenues through online channels
Regionally, risk verification is the most common concern for Omni-Retailers and e-Commerce merchants that sell digital goods/services.

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

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

- Verification of Customer Identity: 71%
- Excessive Manual Reviews: 26%
- Phone Verification: 25%
- Challenges in Acceptance of International-Based Payment Methods: 25%
- Balancing Fraud Prevention w/Customer Experience: 24%
- Email or Device Verification: 23%
- Inability to Determine Source/Origination of Transaction: 22%
- Inability to Distinguish Between Legitimate Human & Malicious Bot Transactions: 22%
- Emergence of New and Varied Payment Methods: 20%
- Address Verification: 17%

51% of those ranking identity verification as a challenge attribute this to a lack of specialised fraud prevention tools for international orders; 49% to limited/no real-time transaction tracking tools; 48% to the rise of synthetic identities; 47% to balancing the speed of approval against customer friction/abandonment; 41% to the use of mobile for transactions.
5 Businesses are not fighting fraud in an effective way.
A majority report that they track fraud costs by channel and payment method.

- However, only 57% appear to be tracking successful fraud transactions by both channel and payment method.
- Not tracking successful and prevented fraud transactions by both channel and payment method leaves businesses vulnerable to fraudsters, particularly within the online and mobile channels, where fraudsters are adept at testing for weaknesses.

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

- 83% Tracks by Both Channel & Payment Method
- 81% Tracks by Neither
- 70%

**% Tracking SUCCESSFUL and/or PREVENTED Fraud Transactions**

- 59% Track Prevented
- 62% Track Successful

- 69% Tracks Successful Transactions by Both Channel & Payment Method
- 62%
Less than 40% of transactions are flagged by an automated system.

> And among those that are, 60% are sent for manual review.

> And manual reviews aren’t preventing false positives. Just over one-third of declined transactions turn out to be false positives. This has cost and revenue implications, as well as longer-term customer relationship consequences.
The use of more advanced fraud mitigation solutions is limited.
An average of 5.6 fraud mitigation solutions are being used across the surveyed industries.

» However, the use of more sophisticated solutions to address the emerging multi-faceted nature of fraud is limited, particularly with regard to behavioural biometrics and other digital identity solutions that can fight synthetic identity fraud and botnet attacks. Given similar incidence rates between some of the physical (cheque verification, government issued ID) and digital solutions (real-time fraud detection), this suggests some layering of solutions for more effective fraud detection. However, there is still a significant portion of merchants/businesses who are not doing so.

» The use of solutions to address mobile threats (digital identity, geolocation, OTP/2 factor) is limited. And whilst solutions are a sizeable portion of fraud mitigation budgets, manual reviews are one-fifth of costs, further suggesting that current fraud prevention attempts are lacking.

**Fraud Mitigation Solutions Use (Avg. 5.6 Solutions Used)**

- **Basic Verification & Transaction Solutions**
  - Cheque Verification: 42%
  - Authenticate Using Payment Instructions: 36%
  - Name Address DOB Verification: 33%
  - Passive & Negative Lists: 29%
  - Government Issued ID: 43%

- **Advanced Identity Authentication Solutions**
  - Authenticate by Challenge Questions: 31%
  - Authenticate by Quiz or PIN: 49%
  - Authenticate Using Transaction Biometrics: 34%
  - Authenticate Using OTP/2 Factor: 25%
  - Email Risk & Verification: 24%
  - Phone # Risk & Verification: 40%
  - Browser/ Malware Tracking: 43%
  - Geolocation: 31%
  - Digital Identity: 31%

- **Advanced Identity & Transaction Verification Solutions**
  - Real-Time Fraud Detection: 46%
  - Automated Transaction Scoring: 29%

**Distribution of Fraud Mitigation Costs by Percent of Spend**

- Fraud Prevention Solutions: 60%
- Manual Reviews: 20%
- Physical Security: 20%
But it’s not just about the number of solutions. It’s important to layer the right combination to meet threats from specific types of channels and transactions.

» Bundling Digital Identity, Geolocation, and Real-Time Fraud Detection solutions can be an effective fraud mitigation tool.

» Regional findings show that APAC businesses in surveyed industries that do this are better able to address mobile threats and the fast-paced challenge of digital/anonymous transactions, resulting in fewer successful fraudulent transactions and lower fraud costs overall.

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

% of False Positives

<table>
<thead>
<tr>
<th></th>
<th>DOES NOT USE</th>
<th>USES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Identity, Geolocations, and Real-Time Fraud Detection</td>
<td>34%</td>
<td>19%</td>
</tr>
</tbody>
</table>

LexisNexis Fraud Multiplier℠

<table>
<thead>
<tr>
<th></th>
<th>DOES NOT USE</th>
<th>USES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Identity, Geolocations, and Real-Time Fraud Detection</td>
<td>2.81 times face value of lost transaction</td>
<td>3.82 times face value of lost transaction</td>
</tr>
</tbody>
</table>
Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria as well as both identity and transaction risk.

**Fraud Issues**

- **Digital Goods & Services**: fast transactions, easy synthetic identity and botnet targets; need velocity checking to determine transaction risk along with data and analytics to authenticate the individual.
- **Account-related fraud**: breached data requires more levels of security, as well as authenticating the person from a bot or synthetic ID.
- **Synthetic identities**: need to authenticate the whole individual behind the transaction in order to distinguish from fake identity based on partial real data.
- **Botnet attacks**: mass human or automated attacks often to test cards, passwords/credentials or infect devices.
- **Mobile channel**: source origination and infected devices add risk; mobile bots and malicious malware makes authentication difficult; need to assess the device and the individual.

**Solution Options**

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

- **Authenticating the physical person**
  - **Basic Verification**: verifying name, address, DOB or providing a CVV code associated with a card (Solution examples: cheque verification services; payment instrument authentication; name/address/DOB verification).
  - **Active ID Authentication**: use of personal data known to the customer for authentication; or where user provides two different authentication factors to verify themselves (Solution examples: authentication by challenge or quiz; authentication using OTP / 2 factor).

- **Authenticating the digital person**
  - **Digital identity / behavioural biometrics**: analyses human-device interactions and behavioural patterns such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognising normal user and fraudster behaviour (Solution examples: authentication by biometrics; e-mail/phone risk assessment; browser/malware tracking; device ID / fingerprinting).
  - **Device assessment**: uniquely identify a remote computing device or user (Solution examples: device ID / fingerprint; geolocation).
Recommendations

Technology is the Key

» To minimize fraud, organizations can no longer rely on manual processes with the assistance of limited technologies to reduce challenge rates, manual reviews, and costs.

» Businesses need a robust fraud and security technology platform that helps them adapt to a changing digital environment, offering strong fraud management and resulting in a frictionless experience for genuine customers.

» Deploying technologies, which can recognize customers, pinpoint fraud, and build the fraud knowledge base to streamline onboarding, can prevent account takeovers and detect insider threats.

» Using valuable data attributes like users’ login from multiple devices, locations, and channels is essential for identifying risks.

» Enabling integrated forensics, case management, and business intelligence can help to improve productivity.
**Recommendations**

**Multi-Layered Fraud Defense is Required**

» Single point protection is no longer enough and results in single point of failure.

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

» A multi-layered, strong authentication defense approach is needed. This includes a single authentication decision platform that incorporates real-time event data, third-party signals, and global, cross-channel intelligence.

» Also required is the ability to examine malware level threats, Bot, and remote access Trojan and IP spoofing detection across web and mobile channels.

» At the same time, the ability to provide behavioral analytics and reduce false positives and customer friction is key.
Recommendations

**Improve Decisioning With Machine Learning**

» Employing machine technology will further reduce fraud mitigation costs and manpower by adapting to changing customer behaviors over time.

» Organisations that have existing fraud detection policies can test different machine learning models until they find one that best aligns with their business objectives.

» Such a model can deliver benefits that include enhanced fraud detection, reduction in false positives, improved identification of trusted customers, and optimized challenge and maximum review rates.
Recommendations

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/geometry
LexisNexis® Risk Solutions can help

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

### Identity Verification
- Validate name, address and phone information
- Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages
- Perform global identity checks with seamless integration and reporting capabilities

### Transaction Risk Scoring
- Identify risks associated with bill-to and ship-to identities with a single numeric risk score
- Quickly detect fraud patterns and isolate high-risk transactions
- Resolve false-positive and Address Verification Systems failures

### Manual Research Support
- Access billions of data records on consumers and businesses
- Discover linkages between people, businesses and assets
- Leverage specialised tools for due diligence, account management and compliance

### Identity Authentication
- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenario
- Receive real-time pass/fail results

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

« These businesses experience high successful fraud volumes and transactions amounts, even though they are using just as many fraud mitigation solutions, on average, than others.

» Financial Services businesses also attribute more fraud losses to identity fraud and are more likely to rank identity verification as a challenge than other businesses.

<table>
<thead>
<tr>
<th>Region Overall</th>
<th>Industry</th>
<th>Offer m-Commerce</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Retail</td>
<td>e-Commerce</td>
</tr>
<tr>
<td>LexisNexis Fraud Multiplier℠</td>
<td>3.40</td>
<td>2.80</td>
</tr>
<tr>
<td>Fraud Costs as % of Revenues</td>
<td>1.75%</td>
<td>1.64%</td>
</tr>
<tr>
<td>Avg. # Fraud Mitigation Solutions</td>
<td>5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Avg. # SUCCESSFUL Monthly Fraud Transactions</td>
<td>391</td>
<td>305</td>
</tr>
<tr>
<td>Avg. $ Amount of SUCCESSFUL Monthly Fraud Transactions</td>
<td>RM 1,755</td>
<td>RM 1,425</td>
</tr>
<tr>
<td>% of m-Commerce That Offer Mobile Apps</td>
<td>95%</td>
<td>93%</td>
</tr>
<tr>
<td>% Distribution of Losses Related to Identity Fraud</td>
<td>33% (14% synthetic)</td>
<td>27% (9% synthetic)</td>
</tr>
<tr>
<td>% Ranking Identity Verification as a Top Online/Mobile Challenge</td>
<td>65%</td>
<td>58%</td>
</tr>
</tbody>
</table>
And when looking within industries, it is digital goods merchants and digital Financial Services businesses that get hit hardest by fraud.

- Digital goods account for nearly a half of Retail/e-Commerce fraud losses, whilst the online/mobile channels account for nearly two-thirds of Financial Services fraud losses.

- These businesses have higher successful fraud volumes and values than others, which contributes to higher fraud costs.

- Businesses that are digital in nature (either by type of good sold or transaction channel) are highly likely to allow transactions through high-risk mobile apps, which further compounds the challenges faced regarding identity verification, including synthetic identities.

<table>
<thead>
<tr>
<th></th>
<th>Retail/e-Commerce</th>
<th>Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LexisNexis Fraud Multiplier℠</strong></td>
<td>Sell digital goods*</td>
<td>3.09</td>
</tr>
<tr>
<td></td>
<td>Sell physical goods only</td>
<td>2.71</td>
</tr>
<tr>
<td><strong>Fraud Costs as % of Revenues</strong></td>
<td>2.45%</td>
<td>1.56%</td>
</tr>
<tr>
<td><strong>% Fraud Losses From…</strong></td>
<td>Digital goods = 39%</td>
<td>Online/mobile channels = 62%</td>
</tr>
<tr>
<td><strong>Avg. # Fraud Mitigation Solutions</strong></td>
<td>5.8</td>
<td>5.2</td>
</tr>
<tr>
<td><strong>Avg. # SUCCESSFUL Monthly Fraud Transactions</strong></td>
<td>443</td>
<td>156</td>
</tr>
<tr>
<td><strong>Avg. $ Amount of SUCCESSFUL Monthly Fraud Transactions</strong></td>
<td>RM 1,687</td>
<td>RM 1,205</td>
</tr>
<tr>
<td><strong>% of m-Commerce ThatOffer Mobile Apps</strong></td>
<td>98%</td>
<td>88%</td>
</tr>
<tr>
<td><strong>% Distribution of Losses Related to Identity Fraud</strong></td>
<td>31% (13% synthetic)</td>
<td>25% (8% synthetic)</td>
</tr>
<tr>
<td><strong>% Ranking Identity Verification as a Top Online/Mobile Challenge</strong></td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td><strong>% Ranking Synthetic Identities as Top Challenge to Identity Verification</strong></td>
<td>48%</td>
<td></td>
</tr>
</tbody>
</table>
 Fraud is also sizeable across APAC countries.

<table>
<thead>
<tr>
<th>Region Overall</th>
<th>Singapore</th>
<th>Indonesia</th>
<th>Malaysia</th>
<th>Philippines</th>
</tr>
</thead>
<tbody>
<tr>
<td>LexisNexis Fraud Multiplier℠</td>
<td>3.40</td>
<td>3.45</td>
<td>3.25</td>
<td>3.57</td>
</tr>
<tr>
<td>Fraud Costs as % of Revenues</td>
<td>1.75%</td>
<td>1.57%</td>
<td>1.66%</td>
<td>1.93%</td>
</tr>
<tr>
<td>Avg. # Fraud Mitigation Solutions</td>
<td>5.5</td>
<td>5.4</td>
<td>5.6</td>
<td>5.6</td>
</tr>
<tr>
<td>Avg. # SUCCESSFUL Monthly Fraud Transactions</td>
<td>391</td>
<td>317</td>
<td>464</td>
<td>401</td>
</tr>
<tr>
<td>Avg, $ Amount of SUCCESSFUL Monthly Fraud Transactions</td>
<td>RM 1,755</td>
<td>RM 1,785</td>
<td>RM 1,806</td>
<td>RM 1,894</td>
</tr>
<tr>
<td>% of m-Commerce That Offer Mobile Apps</td>
<td>95%</td>
<td>92%</td>
<td>98%</td>
<td>93%</td>
</tr>
<tr>
<td>% Distribution of Losses Related to Identity Fraud</td>
<td>33% (14% synthetic)</td>
<td>34% (14% synthetic)</td>
<td>34% (13% synthetic)</td>
<td>31% (15% synthetic)</td>
</tr>
<tr>
<td>% Ranking Identity Verification as a Top Online/Mobile Challenge</td>
<td>65%</td>
<td>65%</td>
<td>62%</td>
<td>68%</td>
</tr>
</tbody>
</table>