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 Indonesian 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 results from the Indonesia market.

<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>TOTAL</td>
<td>90</td>
<td>90</td>
<td>90</td>
<td>90</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

Across various categories, including:  

*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 Indonesia is 3.25 times the lost transaction value. 
   This appears to be driven higher by Financial Services businesses, where the cost of fraud is 3.88 times the value of the lost transaction.

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

3. Customer identity verification is a key issue for online channels. 
   Synthetic identities and botnet attacks are contributing factors.

4. Businesses in surveyed industries that offer m-Commerce suffer from the cost of fraud. But Digital Financial Services firms (regionally) suffer even more. 
   For every fraudulent incident, the cost to businesses that offer m-Commerce is actually 4.01 times the amount of the lost transaction value, totaling fraud costs that are 1.78% 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 optimally fighting fraud. 
   Half do not track successful fraud transactions by both channel and payment method. Additionally, an average of 48% 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 and Geolocation is very limited.
The cost of fraud for surveyed industries in Indonesia is 3.25 times the lost transaction value.
The LexisNexis Fraud Multiplier℠ is 3.25 across surveyed industries.

» This means that for every fraudulent transaction, the cost to Indonesian businesses is actually 3.25 times the amount of the lost transaction value. This translates to fraud costs amounting to 1.66% 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 Indonesia (3.88 times the face value of the lost transaction) than in the United States (2.92 times). Some of this could relate to a 78% year-on-year growth in Financial Services attack rates for new account creations in the region.1

» The mobile channel, digital goods sales, and limited use of solutions to address specific threats are part of the reason for higher risks and costs.

![LexisNexis Fraud Multiplier℠ Chart]

Financial Services businesses experience about 1.5x as many fraudulent transactions and at 2x the monetary amount of Retail and e-Commerce businesses.

---

1 ThreatMetrix® H2 2018 Cybercrime Report
How is the LexisNexis Fraud Multiplier℠ calculated?

**Illustration**
Calculating the LexisNexis Fraud Multiplier℠

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

---

**Step 1:** Obtain average revenue
Rp 4,809,779,532,243*

**Step 2:** Obtain fraud as % of annual revenue from Q10
1.66%

**Step 3:** Calculate total cost of fraud (Steps #1 x #2)**
Rp 79,842,340,235

**Step 4:** Obtain % of total losses for lost transaction values (actual values of the fraudulent transactions that occurred) (Q16)
30.76%

**Step 5:** Calculate actual value of the fraudulent transaction that occurred (Steps #3 x #4)
Rp 24,559,503,856

**Step 6:** Calculate total cost for every S$ 1 of fraud (total cost in Step 3) / (value of fraudulent transactions in Step 5)
$3.25

---

**Note:**
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 Indonesia.

### Market Conditions

The risk of fraud is higher through remote channels and Indonesia's e-Commerce/m-Commerce sectors are thriving & growing:

- e-Commerce has rapidly risen because of increased smartphone use. With more than 40% of its population on smartphones, about 70% of internet traffic comes from these devices.²

- Informal or social commerce accounts for 40% of all digital sales in the country.²

- The number of online sellers in Indonesia has doubled every year for the past three years and reached a total of 4.5 million active sellers in 2017.³

- m-Commerce grew 39% YOY 2017-2018.⁴

- **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.

This increases opportunities for cyberattacks & fraud.

- In 2018, Indonesia had more than 200 million cyberattacks.⁵

- Ranks #9 on the list of 10 worst botnet infected countries.⁶

---

### 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.

---

2 https://theaseanpost.com/article/rise-e-commerce-indonesia
5 http://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009
6 https://www.spamhaus.org/statistics/botnet-cc/
Major revenue and fraud losses come from Indonesia-oriented transactions.

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

» There is a disproportionate degree of fraud from Eastern Asia and Northern/Southern/Western Europe 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.7

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

» Though average mobile channel transaction volumes are modest compared to other types, m-Commerce experienced a ~39% YOY growth from 2017-2018. Over half of study respondents indicate allowing m-Commerce transactions.

» Not surprisingly, millennials are driving the m-Commerce sector. Expectedly, millennials are more likely to shop via mobile devices, than are older generations.8

» Of businesses offering m-Commerce, the largest share 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 level9, 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.

---

8 https://cdn.cms-twdigitalassets.com/content/dam/marketing-
But, mobile channel risk appears to be an accepted trade-off for business grow.

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

- Helps Grow My Business: 65%
- Customer Convenience: 61%
- Need to Remain Competitive: 54%
- Helps Efficient Processing of Applications and Transactions: 44%
- Easier, Faster Customer Experience: 44%
- Meets Customer Expectations of Providing More Engagement: 43%
- Less Expensive to Interact with Customers: 31%
- Reduces Friction of In-Store/Location Waiting: 25%
Traditional payment methods are largely accepted (credit, cash, debit cards), but so too are mobile apps, as businesses strive to reach unbanked customers.

» Less than half of Indonesians are reported to have a bank account, and only 2.4% are reported to have a credit card. Although 56% percent of all Indonesians inhabit large cities and are increasingly living their lives on mobile devices, the other half reside in rural areas and are scattered across 17,000 islands, where cash remains a primary medium of exchange. But with more and more of Indonesia’s 180 million unbanked now using smartphones, a wave of new fintech startups are attacking the space in order to provide them with mobile money and Financial Services.10

» Additionally, informal or social commerce is on the rise. This involves the buying and selling of goods through unofficial means, such as the use of social media and messaging platforms (WhatsApp and Facebook). Unlike in many other countries – especially in the West – informal or social commerce appears to be thriving in Indonesia.11

% 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)

<table>
<thead>
<tr>
<th>=</th>
<th>Debit Transaction</th>
<th>Credit Transaction</th>
<th>Cash</th>
<th>Mobile Wallet Apps (3rd Party &amp; Branded)</th>
<th>3rd Party Payment Providers Such as PayPal, etc.</th>
<th>Gift Cards</th>
<th>Other Alternative Transaction Methods Such as BillMeLater, eCheque</th>
<th>Virtual Currency</th>
<th>Social Media Payments</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>97%</td>
<td>95%</td>
<td>94%</td>
<td>98%</td>
<td>23%</td>
<td>21%</td>
<td>13%</td>
<td>12%</td>
<td>3%</td>
</tr>
</tbody>
</table>

11 https://theaseanpost.com/article/rise-e-commerce-indonesia
Customer identity verification is a key issue for online channels.
Customer identity verification is a key challenge in online channels.

- The sheer growth in Indonesia’s internet economy and mobile transactions undoubtedly contributes somewhat to difficulties in determining if provided information is associated with the identity of a real person.
- Inability to distinguish between human and bot transactions and challenges related to acceptance of international-based transaction methods are also challenging for the mobile channel, whilst address verification and email/device verification are somewhat more challenging for the online channel.

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

*among those transacting through each channel*

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Online Channels</th>
<th>Web Browser</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of Customer Identity</td>
<td>57%</td>
<td>36%</td>
<td>24%</td>
</tr>
<tr>
<td>Inability to Distinguish Between Legitimate Human &amp; Bot Transactions</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Challenges in Acceptance of Int’l-Based Transaction Methods</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Balancing Fraud Prevention &amp; Customer Experience</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Inability to Determine Source/Origin of Transaction</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Address Verification</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Phone Verification</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Email or Device Verification</td>
<td>54%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>Lack of Specialised Tools for Int’l Orders/Transactions</td>
<td>6%</td>
<td>17%</td>
<td>24%</td>
</tr>
<tr>
<td>Excessive Manual Order Reviews</td>
<td>16%</td>
<td>24%</td>
<td>27%</td>
</tr>
<tr>
<td>Assesment of Fraud Risk by Country/Region</td>
<td>7%</td>
<td>5%</td>
<td>15%</td>
</tr>
</tbody>
</table>
Key factors that interfere with effective customer identity verification include balancing speed of approval against customer friction, the rise of synthetic identities, limited ability to confirm order location, and volume of malicious botnet orders.

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 2018.12

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

- Balancing Speed of Approval Against Customer Friction:
  - Web Browser: 49%, Mobile: 53%
  - Web Browser: 39%, Mobile: 54%

- Rise of Synthetic Identities:
  - Web Browser: 44%, Mobile: 48%
  - Web Browser: 48%, Mobile: 45%

- Limited Ability to Confirm Order Location:
  - Web Browser: 48%, Mobile: 50%
  - Web Browser: 41%, Mobile: 50%

- Volume of Malicious Botnet Orders Being Placed at Once:
  - Web Browser: 50%, Mobile: 41%
  - Web Browser: 30%, Mobile: 26%

- Limited/No Access to Real-Time Third Party Data Sources:
  - Web Browser: 45%, Mobile: 41%
  - Web Browser: 48%, Mobile: 41%

- Limited/No Real-Time Transaction Tracking Tools:
  - Web Browser: 48%, Mobile: 41%
  - Web Browser: 30%, Mobile: 26%

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**

<table>
<thead>
<tr>
<th>Extremely Hard to Distinguish from Legitimate Customers</th>
<th>Difficult to detect with traditional identity verification / authentication solutions</th>
<th>Real customers don’t help; behaviours make it difficult to spot anomalies with current ID solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on nurturing the identity to mimic a good customer, establishes good credit, pays on-time, etc. before “breaking bad”</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Many across surveyed industries believe that reducing fraud can help increase revenues and customer loyalty.

» However, there are also expectations that e-gift card fraud will continue to rise, that the mobile channel adds fraud risk, and that fraud is inevitable.

» In 2018 alone, Indonesia experience more than 200 million cyberattacks.\(^\text{13}\)

» This underscores the importance of businesses implementing effective fraud mitigation solutions.

13 http://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009

*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 62%, comes from online channels.

» Mobile transactions in the region are experiencing a growth in attack rate of 17% year-on-year.\(^{14}\)

» Whilst the mobile web browser accounts 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.

\(^{14}\) ThreatMetrix® H2 2018 Cybercrime Report
*% can add to more than 100% since answers based on using a channel
With so much of fraud occurring through online channels, it’s not surprising that approximately 34% of fraud losses are due to identity fraud (3rd party/ synthetic identity) alone.

- 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.  

15 Ibid.
Whilst credit and debit transactions account for the largest individual amounts of fraud losses, alternative and other methods (which include web and mobile options) amount to nearly as much.

» Credit and debit fraud crime is a concern. Much of this type of crime involves dishonest employees of smaller businesses and restaurants copying details of a card or swiping it through a skimmer. This enables them to copy credit card information and make fraudulent cards with valid credit card numbers.16

» Not surprisingly, then, stolen card and CNP make up the majority of fraud losses.

16 https://www.osac.gov/Content/Report/ca756e6a-ce5e-403b-a85e-15f4aeab5362

*% can add to more than 100% since answers based on whether using a channel
62% of businesses across surveyed industries have experienced an increase in automated botnet activity during the past year.

» This is a growth of 14% of transactions on average.
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><strong>» Rise of mobile botnet attacks</strong>; malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases**¹⁷</td>
<td><strong>» Uncertainties, blind spots and new payment methods</strong>; it becomes difficult to determine transaction origination; lack of verifiable data on consumers (particularly with GDPR)</td>
<td><strong>» Fast transaction</strong>; digital goods/services, such as downloads and subscriptions, tend to occur quickly; lack of a physical delivery address eliminates buffer period for fraud verification before shipment; with fear of abandonment, merchants struggle with balancing fraud prevention and minimising customer friction.</td>
</tr>
<tr>
<td><strong>» Consumer risk behaviours</strong> – using open WiFi networks increases risk of smishing (SMS-based phishing) and man-in-the-middle interception of passcodes used for multi-factor authentication¹⁸; “keep me logged in” habits become an unlocked entry point to accounts</td>
<td></td>
<td><strong>» Favourite target for fraudster card testing</strong>; use of bots to test stolen credit card information with lower value goods/services (typical of digital goods/services) tend to arouse less suspicion.</td>
</tr>
<tr>
<td><strong>» Increasing pool for fraudster opportunity</strong> as more people conduct mobile transactions</td>
<td></td>
<td><strong>» Easy targets</strong>; synthetic identities and stolen data make it difficult to distinguish between malicious attacks and legitimate customers in the anonymous channel.</td>
</tr>
</tbody>
</table>

¹⁷ Ibid.
This results in higher volumes and cost of fraud for businesses that offer m-Commerce.

» Every fraudulent transaction actually costs these businesses **4.01 times the value of lost transaction**. This is higher than the average across organisations (3.25) 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>4.01</td>
<td>1.78%</td>
<td>660 Retellers/e-Commerce</td>
</tr>
<tr>
<td>x face value of lost transaction</td>
<td></td>
<td>Rp 7,710,899 Financial Services</td>
</tr>
</tbody>
</table>

* 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 channel itself 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 SM**

<table>
<thead>
<tr>
<th>Retailers/e-Commerce Merchants</th>
<th>Financial Services Businesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Regional Level Across APAC Study Countries)</td>
<td>(Regional Level Across APAC Study Countries)</td>
</tr>
<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>Does NOT Generate Majority of Revenues via Online Channels</td>
</tr>
<tr>
<td>2.71</td>
<td>3.88</td>
</tr>
<tr>
<td>DOES Sell Digital Goods/Services*</td>
<td>DOES Generate Majority of Revenues via Online Channels**</td>
</tr>
<tr>
<td>3.09</td>
<td>4.09</td>
</tr>
</tbody>
</table>

*Does NOT Sell Digital Goods/Services**: Does NOT Sell Digital 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

**Does Generate Majority of Revenues via Online Channels****: Does Generate Majority of Revenues via Online Channels (50% or more of revenues through online channels)

Higher than digital mid/large US Financial Services (2018) (3.18 times)
Regionally, risk verification is the most common challenge 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 the mobile channel (where attack rates are on the rise).

### Top 3 Challenges Related to Selling Digital Goods & Services
(Regional Level Findings)

- **Verification of Customer Identity**: 71%
- **Excessive Manual Reviews**: 26%
- **Phone Verification**: 25%
- **Challenges in Acceptance of International-Based Payment Methods**: 25%
- **Balancing Fraud Prevention Friction 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.
Businesses across surveyed industries are **not** optimally fighting fraud.
A majority are reportedly tracking fraud costs by channel and payment method.

- However, significantly fewer appear to be tracking successful fraud transactions by both channel and payment method.
- It is important to track successful and prevented fraud by both channel and payment method to understand weak points; fraudsters will keep testing for ways to breach systems.

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

<table>
<thead>
<tr>
<th>Tracks by Both Channel &amp; Payment Method</th>
<th>86%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracks by Neither</td>
<td>5%</td>
</tr>
<tr>
<td>By Channel (In-Store, Web Browser, Mobile)</td>
<td>71%</td>
</tr>
<tr>
<td>By Payment Method (Credit/Debit Card, Cheque, etc.)</td>
<td>79%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Track Prevented</th>
<th>Track Successful</th>
</tr>
</thead>
<tbody>
<tr>
<td>59%</td>
<td>58%</td>
</tr>
<tr>
<td>60%</td>
<td>55%</td>
</tr>
</tbody>
</table>

Tracks Successful Transactions by Both Channel & Payment Method: 49%
Less than 40% of transactions are flagged by an automated system.

» And among those that are, nearly half are sent for manual review.

» Unfortunately, manual reviews aren’t preventing false positives, with nearly 1 in 3 transactions (32%) declined in error. This has revenue and 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 behavioral 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, name/address/DOB) 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) is very limited. And whilst solutions are a sizeable portion of fraud mitigation budgets, manual reviews are nearly one-fifth of costs, further suggesting that current fraud prevention attempts are lacking.
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)

<table>
<thead>
<tr>
<th>% of False Positives</th>
<th>LexisNexis Fraud Multiplier&lt;sup&gt;SM&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOES NOT USE</strong></td>
<td><strong>USES</strong></td>
</tr>
<tr>
<td>Digital Identity, Geolocations, and Real-Time Fraud Detection</td>
<td>Digital Identity, Geolocations, and Real-Time Fraud Detection</td>
</tr>
<tr>
<td>34%</td>
<td>19%</td>
</tr>
<tr>
<td>3.82 times face value of lost transaction</td>
<td>2.81 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.

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

<table>
<thead>
<tr>
<th>Solution Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing the transaction risk</td>
</tr>
<tr>
<td>Velocity checks / transaction scoring:</td>
</tr>
<tr>
<td>monitors historical shopping patterns</td>
</tr>
<tr>
<td>of an individual against their current</td>
</tr>
<tr>
<td>purchases to detect if the number of</td>
</tr>
<tr>
<td>orders by the cardholder match up or</td>
</tr>
<tr>
<td>if there appears to be an irregularity (Solution examples: real-time transaction scoring; automated transaction scoring)</td>
</tr>
<tr>
<td>Account authenticating the physical person</td>
</tr>
<tr>
<td>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)</td>
</tr>
<tr>
<td>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)</td>
</tr>
<tr>
<td>Authenticating the digital person</td>
</tr>
<tr>
<td>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)</td>
</tr>
<tr>
<td>Device assessment: uniquely identify a remote computing device or user (Solution examples: device ID / fingerprint; geolocation)</td>
</tr>
</tbody>
</table>
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.
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/geography
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>% 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>LexisNexis Fraud Multiplier℠</th>
<th>Retail/e-Commerce</th>
<th>Financial Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sell digital goods*</td>
<td>Sell physical goods only</td>
</tr>
<tr>
<td>LexisNexis Fraud Multiplier℠</td>
<td>3.09</td>
<td>2.71</td>
</tr>
<tr>
<td>Fraud Costs as % of Revenues</td>
<td>2.45%</td>
<td>1.56%</td>
</tr>
<tr>
<td>% Fraud Losses From…</td>
<td>Digital goods = 39%</td>
<td>Online/mobile channels = 62%</td>
</tr>
<tr>
<td>Avg. # Fraud Mitigation Solutions</td>
<td>5.8</td>
<td>5.2</td>
</tr>
<tr>
<td>Avg. # SUCCESSFUL Monthly Fraud Transactions</td>
<td>443</td>
<td>156</td>
</tr>
<tr>
<td>% of m-Commerce ThatOffer Mobile Apps</td>
<td>98%</td>
<td>88%</td>
</tr>
<tr>
<td>% Distribution of Losses Related to Identity Fraud</td>
<td>31% (13% synthetic)</td>
<td>25% (8% synthetic)</td>
</tr>
<tr>
<td>% Ranking Identity Verification as a Top Online/Mobile Challenge</td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td>% Ranking Synthetic Identities as Top Challenge to Identity Verification</td>
<td>48%</td>
<td></td>
</tr>
</tbody>
</table>
Fraud is also sizeable across APAC countries.

<table>
<thead>
<tr>
<th><strong>Region Overall</strong></th>
<th><strong>Country</strong></th>
<th><strong>Singapore</strong></th>
<th><strong>Indonesia</strong></th>
<th><strong>Malaysia</strong></th>
<th><strong>Philippines</strong></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>
<td>3.46</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>
<td>2.03%</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>
<td>5.1</td>
</tr>
<tr>
<td>Avg. # SUCCESSFUL Monthly Fraud Transactions</td>
<td>391</td>
<td>317</td>
<td>464</td>
<td>401</td>
<td>332</td>
</tr>
<tr>
<td>Avg, $ Amount of SUCCESSFUL Monthly Fraud Transactions</td>
<td>Rp 5,904,101</td>
<td>Rp 6,003,689</td>
<td>Rp 6,074,822</td>
<td>Rp 6,430,491</td>
<td>Rp 5,064,723</td>
</tr>
<tr>
<td>% of m-Commerce That Offer Mobile Apps</td>
<td>95%</td>
<td>92%</td>
<td>98%</td>
<td>93%</td>
<td>94%</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>
<td>34% (14% 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>
<td>65%</td>
</tr>
</tbody>
</table>
For more information: visit
fraud-and-identity-management