Absorbing indefensible fraud losses to appease consumers ironically costs businesses their brand and customers’ trust.

The results from the latest Experian-IDC study show that the prevailing practice to bear the cost of fraudulent transactions is no longer a solution to mitigating digital fraud risks and losses. Against the rising trend of digitalisation, businesses are challenged to accurately identify and verify the authenticity of digital transactions.

When fraudulent transactions occur, customers fall into what IDC terms as a consumer fraud response cycle. There are 3 dimensions that define this response cycle: their desire for convenience, their propensity to share personal data, and their risk perception.

The reality is that consumers, in the aftermath of fraud incidents, adjust their perceptions and behaviours. Left unmanaged, they are likely to spiral into a vicious response cycle that can counteract the effectiveness of the fraud measures taken by businesses.

The vicious cycle manifests in two ways – further defined by the two consumer clusters that our study identified – Digital Voyagers and Digital Pragmatists. These two groups differ in the ways they make trade-offs; each set of trade-offs is reinforced by differing risk attitudes and perceptions, resulting in two different sets of outcomes: escalating fraud losses as Digital Voyagers increase their digital consumption, or lost revenue opportunities as Digital Pragmatists switch to competitors who do better at fraud management.

This report takes a closer look at how Asia-Pacific businesses fare in fraud management, through their customers’ eyes. We conclude that businesses can, and must, improve user authentication and experience as well as increase verification accuracy through measures such as biometric security and data sharing. To protect brand trust, businesses must adopt a multi-layered fraud management strategy comprising customer engagement, real-time data-centricity, and industrial/regulatory collaboration. The proliferation of digital business models foretells increasing revenue share from digital products and services; those who can forewarn fraud before their customer does, will gain consumer trust and reap the most benefits.

“We do not think there is one single solution to eliminate fraud. Everyone needs to play a part.”

~ Retailer in Asia
UNDERSTANDING DIGITAL CONSUMERS’ ATTITUDES AND BEHAVIOURS TOWARD FRAUD

Through the report’s online survey covering 3,200 respondents across 10 countries in Asia-Pacific, we identified 9 behavioural characteristics and 3 dimensions relating to fraud incidence and fraud mitigation strategies.

**DESIRE FOR CONVENIENCE**
Consumers’ choice of channel hinges on the convenience and security factors as well as user experience.
- Consumption of digital services
- Adoption of mobile payment
- Adoption of biometrics for commercial use

**PROPENSITY TO SHARE DATA**
The more loosely personal information is shared, the more susceptible consumers are to data leaks and identity theft.
- Receptiveness to use personal information for fraud detection
- Receptiveness to reuse personal data between businesses
- Quality of data submitted

**RISK PERCEPTION**
Consumers who have experienced fraud — directly or indirectly — are more likely to stay away from unsecured transaction environments.
- Guardedness against personal data at risk
- Tolerance to fraud incidence
- Perceived effectiveness of how organisations handle fraud
The report also draws correlation between the 9 consumer behavioural characteristics and fraud occurrence: 70% or higher reflects a high level of correlation but does not necessarily mean causation. There is a two-way dynamic relationship between consumers’ actions and fraud risk exposure in that consumer actions can affect one’s level of fraud exposure, and conversely fraud exposure can also trigger consumer behaviours.

The interplay of the 3 dimensions further illustrates the consumer fraud response cycle, providing businesses with a holistic view of how consumers’ attitudes in one dimension drives behaviours in the others.
DIGITAL VOYAGERS AND DIGITAL PRAGMATISTS

Further analysis of the consumer fraud response cycle revealed two consumer segments.

The behavioural differences of Digital Voyagers and Digital Pragmatists — and how they result in higher or lower fraud exposure — help businesses understand the effectiveness of their fraud mitigation strategies. We will delve into the 3 dimensions in the following sections.
THE TRADE-OFFS IN CONSUMER DECISION-MAKING

Digital Voyagers and Digital Pragmatists differ in their trade-off decisions along the 3 dimensions of the fraud response cycle. Digital Voyagers’ desire for convenience outweigh their fraud risk perceptions, while a high fraud risk perception drives risk avoidance in Digital Pragmatists.

**DIGITAL VOYAGERS**

- Desire for convenience
  - Higher consumption of digital services
  - Higher adoption of mobile payment
- Propensity to share personal data
  - Higher willingness to share data to get better experience
  - Lower quality of submitted data
- Risk perception
  - Lower tendency to switch providers in the event of fraud

**DIGITAL PRAGMATISTS**

- Desire for convenience
  - Fraud is not acceptable
  - Higher tendency to switch providers in the event of fraud
- Propensity to share personal data
  - Lower willingness to share data to get better experience
  - Higher quality of submitted data
- Risk perception
  - Lower consumption of digital services
  - Lower adoption of mobile payment

How Digital Voyagers and Digital Pragmatists behave point to unsustainable business economics. How businesses manage fraud in accordance to these 3 dimensions affect their ability to balance between fraud management effectiveness and maximising revenue potential. Neglect in one or more of these dimensions triggers one of the two cycles of fraud responses.
While the survey results also reveal general segmentation at a country level (Japan, New Zealand, Australia, Hong Kong and Singapore as Digital Pragmatists; Thailand, China, India, Indonesia and Vietnam as Digital Voyagers), the two segments are in essence a continuum of shifting consumer behaviours within the consumer fraud response cycle. The reality is that consumers shift between the two segments, varying by context.

Like seafaring pioneers, Digital Voyagers explore and seek discoveries before eventually settling down in new lands as Digital Pragmatists.
DESIRE FOR CONVENIENCE

The convenience dimension is represented by three behaviours: consumption of digital services, perceived convenience of mobile payment, and biometric adoption.
THE INTERPLAY OF CONVENIENCE AND FRAUD

The more consumers choose convenience through digital channels, the greater is the fraud exposure for both consumers and businesses.

Consumers who have higher fraud exposure (Digital Voyagers) also have a higher propensity to adopt convenient security measures such as biometrics. This points to opportunities for businesses to improve their fraud mitigation measures.

Where Digital Voyagers and Digital Pragmatists differ

We asked respondents about:
1. Their purchase frequency of groceries, F&B, beauty, fashion, electronics, travel, app downloads and improvement items via online channels.
2. Their frequency of adoption of micro/mobile payment solutions such as contactless cards and in-app mobile wallets.
3. Their openness to using biometrics such as fingerprint, face recognition and iris scanning for user authentication.
HIGHER DIGITAL CONSUMPTION: A CALCULATED RISK

Increasing digital transactions translates into increasing fraud exposure for businesses. In the case of fraudulent transactions, consumers are often covered through chargeback protection, which transfers the fraud loss to either the issuing banks, payment processors or retailers (liability shift rules vary with mode of payment).

With consumers expecting counterparty businesses to be responsible for fraudulent transactions, implicitly, businesses become responsible for the increasing fraud exposure which consumers open themselves to.

Aside from the financial impact, one Chinese online retailer notes “there is impact on brand reputation as fraud happens when consumers are transacting through our Web site”.

The rise of the Next Billion consumers in emerging Asia and the associated surge in mobile Internet connections continue to alter shopping patterns in the region. Vietnam is aiming to reduce cash transactions to become a 90% cashless economy by 2020. The nation has its work cut out for itself as it navigates the complexities and challenges of creating sustainable and secure digital payments.

We asked respondents about:
1. Their online purchase frequency of groceries, F&B, beauty, electronics, travel, and app downloads
2. Their direct/indirect encounters with fraud in the past 12 months

28% of respondents in Vietnam have experienced fraud compared to 6% in Japan.

Consumption of digital services
Fraud experienced

Japan  New Zealand  Australia  Hong Kong  Singapore  Thailand  China  India  Indonesia  Vietnam
FRICIONLESS PAYMENTS FOR A BETTER CUSTOMER EXPERIENCE?

Across the region, 63% of those who have adopted mobile payments consider such payment options highly convenient. Mobile payment adoption is markedly higher in developing markets due to the accessibility and convenience afforded by mobile services such as online ticketing, mobile gaming, bill payment, fund transfers, ride-hailing, and food delivery.

To encourage market penetration, many digital platform businesses have launched accompanying payment wallets for a seamless payment experience. In particular, consumers in developing markets are early adopters of digital wallets; for the unbanked segment, it is one of the limited means to access digital products and services.

Positive outlook for mobile wallets

Sharing economy services and new mobile payments options will grow in tandem as consumers demand a seamless payment experience and countries across the region strive to become cashless economies.

IDC: eWallet solutions are expected to be the fastest-growing and most important form of online payment in the years ahead. In Southeast Asia alone, eWallet gross transaction value (GTV) is expected to grow from US$6.5 billion in 2016 to US$24.4 billion in 2021, at a CAGR of over 30.3%.

1 Source: Tencent Research Institute’s 2017 Mobile Payment Usage in China Report
2 Source: WeChat Website
WHAT’S THE VALUE CONSUMERS PLACE ON CONVENIENCE?

With mobile spending limit expressed as a percentage of average monthly income, we see that **Digital Pragmatists tend to weigh fraud safety over convenience** by limiting their mobile spend.

Increasing consumers' wallet share requires businesses to address two factors simultaneously:

- Providing convenience and improving the user experience
- Alleviating consumers’ risk perception

### Spending limit as a percentage of monthly income

<table>
<thead>
<tr>
<th>Country</th>
<th>Average Monthly Income</th>
<th>Spending Limit as a Percentage of Monthly Income</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vietnam</td>
<td>$131</td>
<td>2.8%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>$89</td>
<td>51.4%</td>
</tr>
<tr>
<td>Thailand</td>
<td>$140</td>
<td>25.1%</td>
</tr>
<tr>
<td>China</td>
<td>$97</td>
<td>13.5%</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>$126</td>
<td>3.5%</td>
</tr>
<tr>
<td>Australia</td>
<td>$143</td>
<td>3.2%</td>
</tr>
<tr>
<td>Singapore</td>
<td>$131</td>
<td>2.8%</td>
</tr>
<tr>
<td>Japan</td>
<td>$92</td>
<td>2.8%</td>
</tr>
</tbody>
</table>

Despite their higher average income levels, **Digital Pragmatists have not increased their wallet share through digital products and services.**

---

1 Spending limit per mobile transaction and monthly income converted to US dollars
ENCOURAGING SIGNS FOR BIOMETRICS

Emerging biometric security solutions are designed to address both areas of improved user experience and stronger authentication, but are consumers willing to adopt the technology?

Almost 4 times as many consumers (57%) are comfortable to use biometrics security in government/noncommercial applications than commercial ones.

Nearly twice as many Digital Voyagers (17%) than Digital Pragmatists (9%) are comfortable to use biometrics security in commercial applications. This spells opportunities for businesses to:

- Partner with trusted governmental agencies in the use of national IDs for user authentication and verification. There are at least 6 national ID projects happening across Asia-Pacific to date.
- Leverage on early adopter consumer attitudes toward biometrics. For example, Citi Hong Kong launched a voice biometrics authentication feature for its consumer banking clients, while Alibaba is piloting facial recognition-based payments in China.

Countries where consumer respondents are more ready to adopt biometrics in commercial applications

- India: 21%
- China: 18%
- Vietnam: 18%
- Thailand: 15%
- Indonesia: 11%
- Digital Pragmatists: 9%

Guangzhou, China:
All eyes are on a new digital ID project backed by China’s Ministry of Public Security. The ambitious project set to roll out in 2018 will pave the way for 13.5 million residents of Nansha District in Guangzhou to use smartphones and facial recognition technology to link their national ID cards with their WeChat accounts.
PROPENSITY TO SHARE PERSONAL DATA

We look at consumers’ risk perception when it comes to sharing personal data and how it relates to fraud.
Consumers are willing to share accurate personal data if they see enough value to justify the disclosure. The persistence of intentional nondisclosures and data errors indicates that businesses need to view data as strategic assets. Increasingly, customer data may not come “free”, either in the form of data cleansing cost, or cost to acquire these data from third parties.

Where Digital Voyagers and Digital Pragmatists differ

We asked respondents about:

1. Their willingness to reuse existing personal data with other business entities.
2. Their willingness to use existing personal data for better fraud management
3. Whether they have made a mistake when submitting personal data (e.g., age, gender, marital status, and income level)
TO SHARE OR NOT TO SHARE?

What do consumers feel about reusing their existing digital accounts?

78% of consumers are open to reuse their personal data when transacting with new businesses, with Digital Voyagers showing higher propensity to do so.

Specifically, they are most agreeable to reuse existing digital accounts for businesses with prevailing relationships. For example, reusing their account information from one bank with another bank.

In addition, when reusing their ID from government e-services, consumers are most comfortable with banks receiving their information held at government agencies.

Consumers’ risk perceptions around data privacy are reduced when:
- There is a credible stake-holding business with which they have existing relationships with, AND
- Consumers deem the information exchange to be used fair in exchange for relevant products and services.

The increased reuse of personal data between businesses of the same type helps validate the efforts of businesses looking at or investing in the use of blockchain and open API technology in further fortifying the trust to businesses through technologies.
CONSUMERS ARE SELECTIVE ABOUT WHAT THEY SHARE AND WITH WHOM

Consumers place varying degrees of value on their personal information in context to their digital relationship with businesses. In terms of their basic personal data, about 66% of consumers show tendencies to share information with different business types. However, for highly guarded data, and demographic information, the willingness to share markedly drops, while consistently showing more trust towards banks and insurance companies.

Businesses need to communicate value in the exchange of personal information. When requesting for personal information not related to a transaction, consumers should be educated on the information to be used and/or shared with third parties.

Among the three types of businesses, financial services firms are in a better position to implement Super ID for universal authentication. A public-private collaboration could further increase consumer trust.

The PromptPay project in Thailand, spearheaded by the country’s central bank, focuses on the integration of customer bank account numbers with the national identification (ID) and mobile phone numbers.

In Singapore, the Ministry of Finance and the Government Technology Agency (GovTech) have launched MyInfo, a personal data platform that contains government-verified personal details. The Monetary Authority of Singapore (MAS) is embarking on a pilot that will expand the MyInfo service to the financial industry for more efficient know-your-customer (KYC) processes.

1 Basic personal data refers to name, email accounts, and phone numbers
2 Highly guarded personal data refers to biometrics, account numbers and passport numbers.
3 Demographic personal data refers to marital status, income level, age group, and education level.
When it comes to sharing their personal data for fraud detection, both Digital Voyagers and Digital Pragmatists recognise its value. However, more Digital Voyagers can readily see value in data reuse to combat fraud.

Consumers who face larger threats from fraudsters are more willing to exchange personal information to fight fraud together with businesses. Organisations should leverage Digital Voyagers’ openness to drive data-driven fraud detection measures.

We asked respondents to rate their level of acceptance to share their personal data with business entities (banks, telecom providers, and retailers) in exchange for different services. (1: Strongly unacceptable, to 4: acceptable, and 5: strongly acceptable)

<table>
<thead>
<tr>
<th>Service</th>
<th>Acceptance Level 4 or 5</th>
<th>Asia-Pacific Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation of new services</td>
<td>41%</td>
<td>43%</td>
</tr>
<tr>
<td>Personalised recommendations and offers</td>
<td>36%</td>
<td></td>
</tr>
<tr>
<td>Personalised experiences (service, time, venue)</td>
<td>33%</td>
<td></td>
</tr>
<tr>
<td>Accurate profiling for fraud detection</td>
<td>43%</td>
<td></td>
</tr>
</tbody>
</table>

% of respondents willing to share their personal data for... (acceptance level 4 or 5)

<table>
<thead>
<tr>
<th>Country</th>
<th>Acceptance Level 4 or 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>56%</td>
</tr>
<tr>
<td>Thailand</td>
<td>51%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>50%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>45%</td>
</tr>
<tr>
<td>India</td>
<td>53%</td>
</tr>
<tr>
<td>Australia</td>
<td>41%</td>
</tr>
<tr>
<td>New Zealand</td>
<td>37%</td>
</tr>
<tr>
<td>Singapore</td>
<td>36%</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>31%</td>
</tr>
<tr>
<td>Japan</td>
<td>19%</td>
</tr>
</tbody>
</table>
CONSUMERS: A SOURCE OF SELECTIVE TRUTH

About 5% of consumers have intentionally submitted inaccurate information to avoid information disclosure, while 20% of respondents have made errors in their data submission, including basic personal data, highly guarded personal data, and demographic data.1

Consumers’ intentional non-disclosure of information exacerbates businesses’ challenge in accurately verifying genuine customers and identifying imposters and fraudsters. In the fight against fraud, businesses must explore third-party sources of consumer data to improve customer verification accuracy.

Intentional non-disclosure: Consumers in Japan (8%) most guarded compared to rest of countries (4-7%)

Data input errors are higher in Thailand, Indonesia and Vietnam
RISK PERCEPTION

Fraud is unacceptable, yet consumers tolerate it. What are consumers’ view of fraud and what are their risk perceptions?
THE SHIFTING LINE OF DEFENCE

The discrepancies between consumers’ fraud expectations and reactions highlight the continuous trade-offs between convenience and fraud risk.

In dealing with **Digital Pragmatists**, businesses have a lower margin of error. Despite absorbing reported fraud losses, there is still risk of losing customers as they are more likely to switch providers when fraud occurs.

With **Digital Voyagers**, their coping mentality signifies a risk transfer from consumers to businesses that continue to absorb fraud losses due to indefensible chargeback claims. **Without effective fraud mitigation measures** to handle digital transaction growth, **businesses risk higher incidence and value of fraud losses**.

Where Digital Voyagers and Digital Pragmatists differ

We asked respondents about:

1. Their tolerance of fraud and the likelihood of switching to another service provider after encountering fraud incidents
2. Their perceptions of how retailers, telecom providers, and financial services firms manage fraud incidences
3. Their concerns about the possible exposure of personal data to fraudsters when engaging in digital activities over public networks (e.g. WiFi)
IN THE ABSENCE OF ALTERNATIVES

Fraud is unacceptable, yet consumers tolerate it. A majority (82%) of respondents find fraud unacceptable, yet in the event of fraud, only 51% will switch or cancel with their current service providers – showing that consumers are tolerating fraud despite their perceptions about it.

In addition, fraud tolerance coincides with higher exposure to fraud incidents. In general, Digital Voyagers have higher fraud tolerance, accompanied with higher fraud exposures.

We asked respondents their acceptance level of fraud occurrence with retailers, telcos, and banks/insurance companies (Note: fraud tolerance sum more than 100% as question repeats across different business types)

1 Respondents’ personal fraud encounter(s), or through family and friends in the last 12 months.

Fraud tolerance with retailers
Fraud tolerance with telcos
Fraud tolerance with banks
Fraud incidents

1We asked respondents their acceptance level of fraud occurrence with retailers, telcos, and banks/insurance companies (Note: fraud tolerance sum more than 100% as question repeats across different business types)

2Respondents’ personal fraud encounter(s), or through family and friends in the last 12 months.
HOW CONSUMERS VIEW FRAUD MANAGEMENT COMPETENCIES

How effective are businesses’ fraud management, really? Less than half or 48% of Asia-Pacific consumers are satisfied with the way businesses have handled fraud incidents.

Consumers’ perceived effectiveness of how businesses handle fraud among Digital Voyagers and Digital Pragmatists

In another survey, businesses rated themselves moderately well in their fraud management capabilities, but regardless of how well they might think they are doing, the message here is that businesses cannot afford to be complacent.

Financial Services

When asked to rate their speed in fraud detection capabilities, financial services firms gave themselves a rating of 3.6 out of 5.

Telco

34% of telecom providers surveyed believe that they do not have a clearly defined ROI for capabilities that provide a single customer view.

Retail

Online retailers rated themselves 3.6 in customer experiences in cases of fraud. Yet incidents and chargeback requests are manually investigated.

Source: Fraud Management Insights 2017
CONSUMER PRECAUTIONARY MEASURES: NON-CONCLUSIVE IMPACT TO FRAUD REDUCTION

When it comes to supplying personal data in a high-risk environment, such as using a public WiFi network, only 19% of respondents would refrain from it, suggesting there is no indication that the level of guardedness has impact on fraud exposure.

Both consumers in Japan (12%) and Indonesia (14%) are the least cautious in providing personal data over public networks. Yet the percentage of Indonesia’s consumers who have experienced fraud is 4 times that of their Japanese counterparts.

Consumers in other countries are more uniform in this regard, at around 21% being cautious when transacting in high-risk environments.

While consumers are an integral part of fraud management, businesses should not depend solely on consumers’ actions but instead take a leading role to minimise fraud occurrences.
WHERE THE DIGITAL VOYAGE ENDS... OR REALLY BEGINS

It's time for a paradigm shift in fraud management.
FROM REACTIVE TO PROACTIVE FRAUD MANAGEMENT

Reactive fraud management does not address consumers’ risk perception and could set businesses into a vicious cycle of high fraud losses and lost business opportunities. That said, our research reveals a silver lining.

Consumers are not only eager to consume digital products and services, they willingly share personal information in support of better fraud management when dealing with trusted entities. This underlines the impetus for businesses to leverage technology to develop a virtuous cycle of trust, data sharing, and increased convenience.

Whether it is biometrics, alternative data services, or blockchain, it is important to recognise that the fraud landscape is constantly evolving, and so are consumer behaviours and expectations.

Different industries face different challenges and consumer expectations. For example, banks are subjected to higher standards of industry regulatory compliance compared to retailers. Online commerce adoption in Australia is high, although consumers remain conservative when it comes to sharing personal data. Disruptive new technology and innovations in areas like mobile payments are also presenting new opportunities and challenges to businesses in ensure secure transactions.

Consumer trust is a direct reflection of a business’ ability to manage and handle fraud. And protecting this trust requires proactive fraud management.

As we have shown in the earlier chapters, a Digital Voyager can behave like a Digital Pragmatist, and vice versa, impacting a business’ ongoing and future revenue.

Managing all the above is equivalent to hitting a moving target, and a silver bullet simply does not exist.
5 BEST PRACTICES OF A MULTI-LAYERED APPROACH

**Adopt a proactive mindset**
Reactive mitigations to fraud is costly and can be disastrous in today’s fast-paced digital economy. The journey begins now as the layers of managing fraud cannot be built overnight.

**Collaborate**
Work with fraud management experts to leverage industry-leading processes and sophisticated tools that can scale to meet increasing fraud threats and business growth (e.g., machine learning and blockchain-based identity management).

**Connect with regulators**
Engage regulators in conversations on regulations and policies that can empower businesses and consumers to prevent fraud.

**Empower your customers**
Technology is only part of the equation when it comes to fraud management. A combination of enabling customers to understand how they can protect themselves to building a relationship of fraud management partnership with transparency.

**Aim for an effective 360-degree view of the customer**
Become customer-centric across multiple channels. Adopt omnichannel aggregation and integration to understand real-time customer transactions.

**Become customer-centric across multiple channels.**
Adopt omnichannel aggregation and integration to support real-time customer transactions.

**Technology is only part of the equation.**
A combination of enabling customers to understand how they can protect themselves to building a relationship of fraud management partnership with transparency.
**IMPETUS TO ACT NOW IN THE FUTURE OF COMMERCE**

Digital native companies such as Lazada, FoodPanda and Traveloka are reshaping consumers’ value perceptions with digital products/services and business model innovations. Beyond traditional products and services, these businesses offer new value propositions – increased convenience, choice, personalisation, and on-demand access to localised products and services – making life simpler and easier for consumers.

IDC expects that by 2019, all digitally transformed organisation will generate at least 45% of their revenue from “Future of Commerce” business models. Consumers’ demand for convenience will continue to grow as they come to trust and depend on these digital services.

**SHIFTING VALUE PROPOSITIONS**

**ECOMMERCE**
- Direct-to-consumer
  - Branded e-Store
  - Online marketplace
- Product accessibility
- Convenience

**DIGITAL COMMERCE**
- Multi-sided value exchange
  - Me-commerce
  - Sharing economy
  - O2O commerce
- Local discovery
- On-demand availability

**FUTURE OF COMMERCE**
- Outcome-based commerce
  - Real-time value chains
  - Information-based products and services
  - Outcome-based monetisation
- 1-to-1 customer relationship at scale

For most organisations, the share of revenue from digital products and services is expected to take on increasing weightage.

Underlying the backdrop of increased convenience and 1-to-1 customer intimacy, is the implicit trust for organisations. Businesses pushing for the penetration of digital product and services must start building on that trust today.

Are you ready with a better response to the consumer fraud challenge?
Experian is the world’s leading global information services company. During life’s big moments – from buying a home or a car, to sending a child to college, to growing a business by connecting with new customers – we empower consumers and our clients to manage their data with confidence. We help individuals to take financial control and access financial services, businesses to make smarter decisions and thrive, lenders to lend more responsibly, and organisations to prevent identity fraud and crime.

We have more than 16,000 people operating across 37 countries and every day we’re investing in new technologies, talented people and innovation to help all our clients maximise every opportunity. We are listed on the London Stock Exchange (EXPN) and are a constituent of the FTSE 100 Index.

Learn more at www.experianplc.com or visit our global content hub at our global news blog for the latest news and insights from the Group.

Contact:

Sean Yeo
T: +65 6593 7597
E-mail: sean.yeo@experian.com
International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

Contact:
Isabelle Chan
T: +65 6829 7757
E-mail: ichan@idc.com