Igniting the Next Frontier in Commerce:
Emerging Digital Commerce Trends in Asia Pacific

February 2013
Abstract

The distinction between the physical and virtual commerce worlds are blurring, giving birth to a new type of commerce: digital commerce. A rising middle class in Asia Pacific, reinforced by a new generation of well-off, young and tech-savvy individuals, high payment card penetration, and a growing willingness to buy online through both mobile and non-mobile platforms are converging to lay the foundation for exponential growth in this exciting market. J Michael Bradley, Managing Director for Asia Pacific, CyberSource, presents the key trends and strategic guideposts to help organisations frame their investment decisions in digital commerce-related initiatives.

Introduction

Commerce trends throughout the Asia Pacific region can be as varied as the countries that make up this vast market. Yet, there are a few common and interrelated trends which point to a profound shift taking place in this space: changing consumer attitudes and purchasing behaviours are transforming the way merchants, financial institutions and even governments are responding in both virtual and physical worlds. At the centre of this shift in the region is an empowered consumer with rising purchasing power, and one who is increasingly connected to the digital world.

Trend 1: The rise of the digitised consumer

How commerce is initiated and transacted today is a truly consumer-centric activity – fueled by rising economic status and greater levels of digital connectivity. Several economic and demographic trends characterise the rise of the digitised consumer in Asia Pacific.

First, there is the inexorable growth of the middle class across many developing markets in the region; the most significant macroeconomic and demographic shifts are occurring in India, China, Indonesia and Vietnam. Currently, the middle class demographic stands at approximately 250-300 million in China, 160 million in India, 50 million in Indonesia and 14.6 million in Vietnam, and is forecast to account for between 46-58 percent of the populations in these countries by 2020. With increasing disposable incomes, this emerging middle class will represent a huge market for digital commerce.

The second driver is the growing proportion of individuals who are connected online. Asia alone makes up almost 45 percent of the world’s Internet users, growing at a compounded rate of 20 percent annually. While Internet penetration as a proportion of population varies across countries – China at 40 percent, India at 11 percent, and Indonesia at 22 percent, just to name three countries – the sheer number of people in the region presents exciting growth opportunities for digital commerce. For instance, the number of Internet users in China alone – at 538 million people – already exceeds the entire population of the USA (which currently stands at 310 million).

The third driver is the rise of the digital native, represented by the “Millennials” (also known as “Gen Y”); highly urbanised individuals who work, play and live just as comfortably online as they do in the physical world. It is estimated that there are 123 million tech-savvy Gen Y individuals in the Asia Pacific region (see table 1), many of whom display consumerist tendencies, as well as the willingness to use cashless payment methods. Currently, 60 percent of Asia Pacific Millennials own at least one credit card, and 80 percent have at least one debit card. Millennials also have a high propensity to shop online: in 11 markets alone, 55 percent indicated they had shopped online.

<table>
<thead>
<tr>
<th>Country</th>
<th>Millennials population</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>49.6 million</td>
</tr>
<tr>
<td>India</td>
<td>35.1 million</td>
</tr>
<tr>
<td>Thailand</td>
<td>1.9 million</td>
</tr>
<tr>
<td>Malaysia</td>
<td>2.0 million</td>
</tr>
<tr>
<td>Vietnam</td>
<td>2.8 million</td>
</tr>
<tr>
<td>Indonesia</td>
<td>5.1 million</td>
</tr>
<tr>
<td>Philippines</td>
<td>2.8 million</td>
</tr>
</tbody>
</table>

Table 1: Millennials by country
Another significant development is the use of mobile devices to support buying decisions and to pay for purchases online. Smartphone use is growing at a rapid pace in the Asia Pacific region: for instance, China’s smartphones users make up 30 percent of all mobile phone users in the country. Out of these, 83 percent use their smartphones to access the Internet, while 43 percent have made a digital purchase via mobile commerce.

A rising middle class reinforced by a new generation of well-off, young and tech-savvy individuals, significant payment card penetration, and a growing willingness to buy online through both mobile and non-mobile platforms are converging to lay the foundation for exponential growth in digital commerce. In markets such as China, eCommerce growth is projected to reach USD 356.1 billion by 2016 (See Figure 1). While China’s eCommerce market is similar in size to the US’s eCommerce market in 2003, it is growing twice as fast, and is expected to become the world’s largest digital commerce market by 2020. Already, merchants, payment service providers and technology vendors are positioning themselves to tap into this opportunity.

![Figure 1: Growth forecasts for eCommerce in selected Asia Pacific markets](image)

**Trend 2: The evolution of credential management in payment infrastructures**

As digital commerce becomes increasingly mainstream, consumer behaviour and expectations are also changing. On one hand, consumers want to transact online in the manner that suits their personal and increasingly mobile lifestyle. Whether it’s via smartphone, laptop or tablet, consumers want the buying and payment experience to be easy to access, understand and complete. Yet, convenience notwithstanding, consumers expect each and every transaction to be secure. In the age of digital commerce, the consumer presumes security and demands convenience for all buying transactions conducted online, regardless of device.

To achieve an optimal balance between these two competing requirements – mobile convenience and security – the market is seeing the rise of several payment technology developments; these include mobile Point-of-Sale (m-POS), mobile wallets (m-wallets) and cloud-based secure storage of payment details and credentials. Simultaneously, we see the interoperability and standardisation of security protocols among mobile devices, payment technologies and networks.

**The push for m-wallets and m-POS deployments**

As the mobile platform becomes the predominant mode of making online purchases, the payment ecosystem has responded by offering two critical innovations: the m-POS terminal and m-wallets. m-POS terminals accept cashless payments via mobile devices, while the m-wallet enables consumers’ bank, credit or debit card account details to be accessed and used as a store of digital currency. Mobile payment technologies are merging with mobile applications to create a richer, more integrated experience for the consumer. To enhance the experience further, additional components such as Radio Frequency Identification (RFID), Near Field Communications (NFC) and Quick Response (QR) code devices can be incorporated into these platforms.

Initiatives are underway across the Asia Pacific region to deploy these new technologies to meet the needs of the untethered consumer. In Thailand, Krungsri Bank, a local financial institution, and Swift, an m-POS payment technology provider, have collaboratively developed m-POS devices in the form of tablet PCs, which are deployed to thousands of AIA insurance agents. Through this payment system, AIA customers can use credit cards issued by Krungsri Bank to pay for insurance premiums through tablet PCs carried by AIA insurance agents in the field.

In China, both m-POS and m-wallet payment infrastructures are proliferating. In Chengdu, China, the municipal government has signed an agreement with China Mobile, the nation’s leading telco, and China UnionPay, to develop the city into a model for mobile payments using m-POS devices. These devices will come in the form of NFC-enabled terminals which China Mobile will deploy. Elsewhere, China Unicom has teamed up with China Merchants Bank to deploy NFC-enabled m-wallets starting with the city of Shanghai.
In the age of digital commerce, the consumer presumes security and demands convenience.

Already, Chinese consumers lead the world in mobile payment adoption, and according to a study, are expected to transact more than CNY 700 billion (USD 112 billion) annually through the mobile platform alone by 2015. The study found that over half (52.14 percent) of Chinese respondents are mobile wallet users compared to a combined total of 12 percent within the other four countries surveyed.

Both emerging mobile payment methods are examples of how the market has responded to the consumers’ need for convenience. Yet, making mobile payment technologies and devices widely available represents only one side of the coin. Ensuring that these payments are secure is the other. The management of sensitive payment data in this new, customer-centric world offers many new complexities. For instance, the demand for convenience and form factor limitations places great strains on the prevailing payment transaction process of entering in full card details into a small screen. In addition, offering a convenient ‘one-stop’ or ‘single-sign-in’ payment process – where existing customer credentials including payment methods are referenced by a unique user name and password – will require a more integrated relationship between the customer, the merchant, banks and payment service providers that make up the payment ecosystem. To address these developments, merchants will need to consider the latest developments in payer authentication methods, as well as payment acceptance and storage.

Tokenisation and secure acceptance

With respect to the credentials used in the payment process, merchants have to grapple with two considerations – how data relating to payment and credentials is stored; and how it is accessed on a regular basis, each time the customer conducts an online transaction.

With tokenisation, sensitive data such as customer credentials are encrypted with unique identifiers or tokens. Tokenisation has taken off because Payment Card Industry Data Security Standards (PCI DSS) no longer allow primary payment card details to be stored “in the clear” on a merchant’s POS terminal or in its databases after a transaction. To be PCI DSS-compliant, merchants will need to invest in and maintain end-to-end encryption systems at high costs – an option which may not be open to many with limited budgets or capabilities.

To overcome this challenge, merchants are opting for payment data to be stored and processed in a third-party PCI DSS-compliant cloud infrastructure. What makes PCI DSS-compliant clouds an attractive proposition are gateway technologies such as secure acceptance. With secure acceptance, payment fields that appear on a merchant’s website are actually hosted on third-party clouds provided by reputable vendors. Sensitive data such as payment data otherwise stored on merchants’ ERP systems will instead be off-loaded to third-party PCI DSS-compliant networks for payment processing, reducing the risks of security breaches.

In such a scenario, the service provider issues the merchant a point-of-sale application which converts credit card numbers into randomly generated values (tokens). Tokenisation, used in conjunction with secure acceptance, makes it more difficult for hackers to gain access to cardholder data, as compared with older systems in which credit card numbers were stored in databases and exchanged freely over networks. Merchant networks only store these tokens – which serve as a proxy for customer credentials – for future transactions or chargeback resolutions.

Trend 3: Increasing maturity in risk management

With various payment methods and platforms contributing to a rapidly evolving digital commerce landscape, managing risks associated with data breaches and fraudulent transaction behaviour becomes more complex. To mitigate them, merchants, system integrators and payment solution providers are turning their attention to improving the authentication process, particularly through the selected use of One-Time Password (OTP) solutions and augmenting authentication through behaviour monitoring.

While OTPs represent a more secure alternative to static passwords, OTPs alone are not foolproof as they are still subject to security breaches, or the algorithm can be compromised. Since OTPs are sent to mobile devices via the Short Message Service (SMS) format, they can also increase the likelihood of a failed transaction in markets that have poor telecommunications infrastructure, or have a high proportion of temporary SIM cards in use.

In order to address the potential shortcomings inherent in password authentication, organisations will need to include a more comprehensive strategy capable of detecting fraudulent behaviour. This is where...
fraud management via **behaviour monitoring** can be leveraged. Behaviour monitoring solutions help paint a picture of the consumer’s true intentions, giving risk administrators an edge in identifying and preempting potentially fraudulent actions. Best-in-class fraud behaviour monitoring technologies analyse hundreds of data points in real-time, while simultaneously checking them against global databases of purchasing history. Purchase patterns can be compiled and compared immediately with past activities, and alerts can be issued if anomalies in usage patterns occur.

In the long term, risk management needs to be viewed through the lens of the market. If it results in slow checkouts, the consumer is more likely to abandon the transaction. From an operational perspective, the cost of implementing payment and risk management solutions will also have to be taken into account. Finally, if the risk management platform itself is too rigid, it may not be able to adapt to changes as a result of evolving customer behaviours, business models and technologies.

**Conclusion**

To fully embrace the rise of the digitised consumer in the Asia Pacific region, businesses will need to consider how the trends expressed in this paper can affect their operations and the customer experience. An optimal risk management strategy in digital commerce can only be achieved through the careful balancing of customer convenience and security. Emerging mobile payment platforms such as m-POS and m-wallets can help streamline the payment process for the consumer; while cloud-based payment acceptance and storage platforms provide the confidence that credentials are retained securely, at a cost that is acceptable to merchants.

As the market evolves, the next frontier of digital commerce will be charted and ignited by those that are ready to tap into the exciting opportunities in the region.

---

**References**

4. ibid
6. ibid
9. ibid

---

**Author: Mr J Michael Bradley**

(Managing Director for Asia Pacific, CyberSource)

Michael is a leading authority on eCommerce fraud, payment security and payment process improvement. A published author on payment and fraud trends, he is a highly sought-after speaker at industry conferences and media events throughout Asia Pacific. Michael collaborates closely with the industry’s largest eCommerce businesses supporting the travel, financial, digital, retail and entertainment segments.
About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 370,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in San Francisco and maintains offices throughout the world, with regional headquarters in Singapore (Asia Pacific), Tokyo (Japan), Miami/Sao Paulo (Latin America and the Caribbean), and Reading, U.K. (Europe/Middle East/Africa). CyberSource operates in Europe under agreement with Visa Europe.

For more information, please visit www.cybersource.com

© 2013 CyberSource Corporation, a Visa company. All rights reserved.