

# ENABLING THE 'CREDENTIAL ECONOMY'

PAYMENT MODELS DRIVING THE DEVELOPMENT OF  
CONSUMER EXPERIENCE IN ECOMMERCE





## ABSTRACT

A new breed of digitally-savvy consumers is driving the development of consumer experience in eCommerce. Critical to the success of this next-generation development will be a frictionless payment experience that mitigates clunky physical interaction, while contributing to loyalty and customer satisfaction. J Michael Bradley, Managing Director for Asia Pacific, CyberSource, examines how the emergence of the ‘Credential Economy’ is taking shape across multiple forms, including digital wallets, micro-transactions and loyalty commerce models. These payment models need to be supported by security solutions designed to protect payment and other Personally Identifiable Information (PII) data. This paper provides an understanding of the credential economy, and offers deeper insights into the various solutions that enable these business models.

### REINVENTING THE CONSUMER EXPERIENCE

The next time you are standing in line to check out of a hotel, ask yourself, “Why am I even here?” Didn’t the hotel already authorise your credit card during check in? Why is there a need to repeat the transaction?

The same questions can apply to a transaction at your local coffee shop, bar, or preferred airline website. We are signing a piece of paper, re-entering credit card details, and waiting while a retailer or a digital process re-acquaints itself with you and your payment details.

Consumers today are aware that the establishment already knows who they are, what services and products they prefer, their reward and loyalty details, and even their credit card details.

Consumer engagement—how individuals shop and transact—will need to start reflecting the focal point of the expected customer experience. Price, quality, and even branding are now under immense pressure to serve as strategic differentiators. At the same time, the ability to provide customers with a smooth, frictionless means of transacting via mobile devices, Point-of-Sale (POS) or websites can further help merchants increase their experiential advantage. In some cases, experiential differentiation could even be the competitive advantage.

Frequent shoppers to well-known websites such as Amazon are familiar with the convenience of their ‘1-click checkout’. With the rise of mobile computing, paper-based signatures and documentation could be replaced by different means of express online checkouts or biometric-based checkout which have the ability to embed within the payment process.

### PAYMENTS AS STRATEGIC DIFFERENTIATOR

We see this development as part of a rapid shift in consumer preference that is fast gaining traction in many growth markets such as China—where payment infrastructures such as China’s Express Checkout<sup>1</sup> are supporting fast and convenient online sales transactions.

However, storing and retaining consumer data can be costly, complex and require companies to comply with evolving regulatory requirements. Organisations need to weigh the costs between that of storing, encrypting and managing systems dedicated to protecting sensitive payment and other Personally Identifiable Information (PII) data, and that of alternative methods of data security such as tokenisation.

**“ We are witnessing a transformation in the payments industry – but this is really a transformation in consumer engagement. ”**

Today, we are beginning to see payments rapidly moving towards this ‘Credential Economy’, where the payment process and the retrieval of payment data does away with the need for actual credit card numbers or PII data. This involves the use of embedded payments, achieved through solutions such as digital wallets, card-on-file and stored values, as well as other payment programme types such as subscriptions and loyalty programmes.

Payment solutions such as Alipay, TenPay and Square are the most visible examples in this sea of change—but they are hardly the only actors in this rapid evolution. The rise of new players, new business models and mobile wallets all speak to the understanding that credentials may become the

new norm for commerce engagement, as consumer experience becomes a strategic differentiator.

There are two main parts to this narrative. The first is to achieve a better understanding of the credential economy. The second is to gain deeper insights into enabling these business models.

## UNDERSTANDING THE CREDENTIAL LANDSCAPE

There is a profound transformation underway for how consumers engage and transact through mobile, eCommerce and POS platforms.

Payments are evolving to be a crucial part of the customer experience. At the heart of this transformation is the use of credentials to identify yourself to the retailer/service provider, and to authenticate your intention to transact. Here, we examine foundational business models developed around this concept of credentials.

### 1. Digital wallets (eWallets)

Digital wallets are consumer-managed digital accounts containing one or more payment instruments. In theory, an eWallet is merchant and brand agnostic, and can be accessed to pay for services and goods universally across a spectrum of businesses. We have, and will continue to see, more examples of eWallets that are focused on specific market segments, geographies and even leveraging mobile networks.

Examples of 'universal' eWallets include PayPal, Google Wallet (Google), Serve (American Express), MasterPass (MasterCard) and Alipay (part of China's Alibaba group). Alipay, in particular, is rapidly gaining traction as a form of payment in eCommerce outside its home market, where it has a 50% market share<sup>2</sup>. There are also mobile eWallets such as ISIS in the U.S. and PeaceSoft in Vietnam.

Credentials are used to access the eWallet to authorise payment, check status or edit the consumer's profile. Sensitive payment data—such as primary account numbers (PANs), bank account information and other critically important PII data—is stored and managed by the wallet providers. However, merchants can still be exposed to sensitive payment data, increasing their risk and costs.

In order for an eWallet to be relevant and support consumer engagement, it must be ubiquitous. Alternatively, it can be highly specialised and focused on a specific market; such as Alipay in China, where the market's size meets the scale criteria.

### 2. Subscriptions

Subscription payment models provide on-going access to goods and services based on persistent relationship

with the service provider. In its simplest form, a provider offers goods or services on a regular or periodic basis (monthly, annually, aggregation).

Subscription-based models have evolved to include irregular micro-transactions (small, irregular purchases such as Apple's iTunes), freemium (common in online gaming, where users enjoy free subscription but only pay for premium upgrades), and usage-based payment models (for example, mobile phone plans).

Subscribers credential themselves in order to authenticate payment or update their profile. All of these variations are consistent in that the provider of the goods and services is required to store consumers' sensitive payment and personal data—and they have to access that information to authorise payment on a regular or irregular basis.

### 3. Top-Up/Stored Value

Another form of payment model is closed-loop, stored-value offerings that help maintain customer loyalty, facilitate 'cash-in' to an ecosystem such as top-up accounts for online gaming or a rail system, or provide another means of customer engagement (for example, gift cards).

Where cash is not the primary source of funds, top-up accounts may be linked to a consumer's payment account such as credit card or bank account. The provider of the top-up account stores sensitive payment information to access that payment credential.

### 4. Loyalty Payment Programme

Loyalty can be considered to be its own industry, let alone a singular topic, when considering the credential economy. However, we are seeing emerging trends where loyalty and payments are linked; innovative providers such as LevelUp in the U.S. or Cellcity in Singapore are enabling physical commerce experiences where combinations of rewards and linkages to consumer payments are creating a high level of engagement for merchants.

Similar to other consumer engagement models, sensitive payment and PII data needs to be stored and subsequently accessed to complete the frictionless experience.

### 5. Card-on-File

A consumer's preferred payment type (cards or debit bank account) is stored along with other PII data, and accessed through a mobile application enabled through the consumer's credentials.

While similar in concept to an eWallet, there is a key distinction: this is a one (merchant) to many (consumers) model, not a many-to-many model, which is the characteristic of an eWallet. We observe that some hotel groups now enable their guests to check out via the card stored on file. Certain quick-service restaurant chains now have mobile apps which allow regular customers to submit their orders from their phone and pick it up at the restaurant—payment is automatically conducted when the consumer enters the store.

## ENABLING THE CREDENTIAL ECONOMY

Now that we have a basic taxonomy of models which underscore the credential economy, businesses can evaluate which approach is right for them. In some cases, organisations may look to leverage multiple credential approaches. A retailer may want to offer multiple payment options, which include various universal wallets; perhaps it will offer its own stored-value gift card or embrace a loyalty payments platform.

Common to all these approaches is the need to cost-effectively and securely manage customers' payment and PII data. The need to consistently upgrade security standards and infrastructure may far outpace any one organisation's ability and appetite to keep abreast.

Using Solution-as-a-Service (SaaS) solutions to address payment security management—what

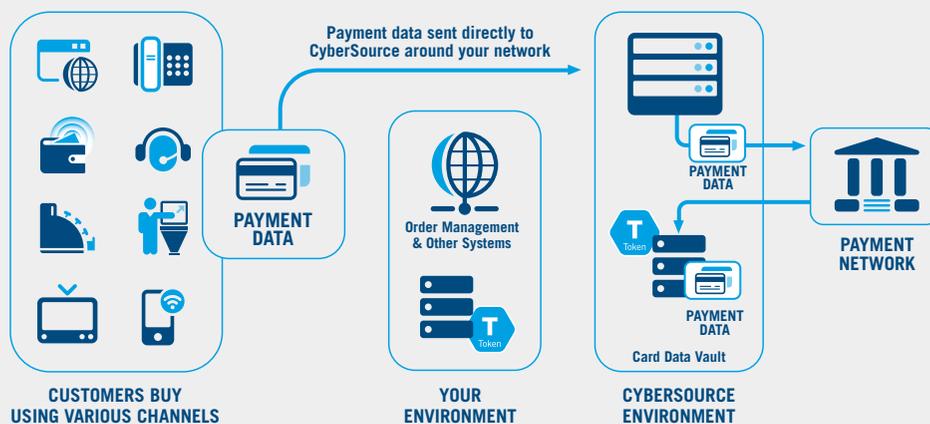
we refer to as tokenisation—may provide greater flexibility and cost efficiencies as compared to in-house solutions. Furthermore, payment security solutions integrated with global payment capabilities offer businesses unparalleled flexibility in how, where, and when to scale their business while managing costs.

Tokenisation is an essential element to secure payment infrastructure and one of the key enablers of the credential economy. It involves the replacement of sensitive data with a unique identifier that cannot be mathematically reversed.

In a merchant's environment, tokens take the place of sensitive credit card data while the data is stored offsite on secure servers owned by the tokenisation service provider. There are multiple token formats generated using proprietary tokenisation algorithms to meet a merchant's business needs.



## HOW CYBERSOURCE TOKENISATION WORKS



The tokenisation process consists of three main phases:

1. When the customer hits the "Submit" button during checkout, all data related to the payment transaction is immediately encrypted and transmitted directly to the tokenisation service provider for processing, token generation and storing. Credit card information never enters the merchant's environment.
2. The encrypted primary account number (PAN) is decrypted when it enters the service provider's Level 1, PCI-compliant data vault, where it is securely stored. The payment data is then passed on to the processing channel (bank) and returned to the service provider with an accepted or denied result.
3. The service provider returns the result to the merchant, but substitutes the PAN data with a uniquely generated token. The merchant stores the token—easily verified with the last four digits of the original PAN retained—in their enterprise resource planning (ERP) system for future transactions or chargeback resolution on that account.

## CREATING A BETTER CONSUMER EXPERIENCE

Ultimately, organisations that are actively invested in facilitating the consumer payment experience may have a competitive advantage. The complexity and costs associated with managing sensitive PII and payment data necessitate the consideration of SaaS-based payment data security models. Whether a business chooses to offer a stored-value wallet, loyalty-based platform, or stored-value payment options, all options underscore the need to handle and/or store sensitive payment data in

accordance with PCI DSS (Payment Card Industry Card Security Standard). Yet, businesses need to excel in the consumer experience, and not just become payment data security experts.

Consumers will continue to place their trust in their favourite hotels, airlines, coffee shops or restaurants. By addressing these strategic opportunities with solution principles that simultaneously embrace robust security, business model flexibility, and cost effectiveness, businesses can continue to fuel their business growth ambitions in a new 'Credential Economy'.



### 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.

---

### Reference

<sup>1</sup>CyberSource, 'The Development of Payments in China's Domestic eCommerce Market: Beyond Express Checkout?', January 2013

<sup>2</sup>China Internet Watch, '10 Charts to Tell You About China Online Shopping Market in Q2 2013', August 2013: <http://www.chinainternetwatch.com/2890/china-online-shopping-q2-2013/>

## About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 400,000 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 Foster City, CA and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami / Sao Paulo and Reading, U.K. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit <http://www.cybersource.com/asiapacific>

### **NORTH AMERICA (US & CANADA)**

#### **CyberSource Corporation HQ**

Phone: 650-432-7350  
Toll Free: 1-800-530-9095  
Email: [sales@cybersource.com](mailto:sales@cybersource.com)  
Website: [www.cybersource.com](http://www.cybersource.com)

### **EMEA (EUROPE, MIDDLE EAST & AFRICA)**

#### **CyberSource EMEA**

Phone: +44 (0)118 990 7300  
Email: [uk@cybersource.com](mailto:uk@cybersource.com)  
Website: [www.cybersource.com/emea](http://www.cybersource.com/emea)

#### **CyberSource Visa Middle East FZ-LLC**

Phone: +971 4 457 7200  
Website: [www.cybersource.com/mea](http://www.cybersource.com/mea)

### **LATIN AMERICA & CARIBBEAN**

#### **CyberSource Miami**

Phone: +1 (305) 328 1998  
Email: [lac@cybersource.com](mailto:lac@cybersource.com)  
Website: [www.cybersource.com/lac](http://www.cybersource.com/lac)

#### **CyberSource Mexico**

Phone: + (52-55) 5387 4185  
Email: [mexico@cybersource.com](mailto:mexico@cybersource.com)  
Website: [www.cybersource.com.mx](http://www.cybersource.com.mx)

#### **CyberSource Brazil**

Phone: +55-11 2102-0088  
Email: [brasil@cybersource.com](mailto:brasil@cybersource.com)  
Website: [www.cybersource.com/brasil](http://www.cybersource.com/brasil)

### **ASIA PACIFIC**

#### **Asia Pacific CYBS Singapore Pte Ltd**

Phone: 001-800-6671-5000 (Singapore / Thailand)  
Phone: 00-800-6671-5000 (Malaysia)  
Phone: 000-800-630-1003 (India)  
Phone: 1-800-8-756-8388 (Philippines – Globe)  
Phone: 1-800-10-802-7222 (Philippines – PLDT)  
Email: [ap\\_enquiries@cybersource.com](mailto:ap_enquiries@cybersource.com)  
Website: [www.cybersource.com/asiapacific](http://www.cybersource.com/asiapacific)

#### **CyberSource KK (Japan)**

Phone: +81 3 3548 9873  
Email: [sales@cybersource.co.jp](mailto:sales@cybersource.co.jp)  
Website: [www.cybersource.co.jp](http://www.cybersource.co.jp)

#### **CYBS Greater China**

Phone: +86 21 6109 5141 /  
+86 21 6109 5100  
Email: [gc\\_enquiries@cybersource.com](mailto:gc_enquiries@cybersource.com)  
Website: [www.cybersource.com/cn](http://www.cybersource.com/cn)

#### **CyberSource Australia & New Zealand**

Phone: 0011-800-6671-5000 (Australia)  
Phone: 00-800-6671-5000 (New Zealand)  
Email: [anz\\_enquiries@cybersource.com](mailto:anz_enquiries@cybersource.com)  
Website: [www.cybersource.com/anz](http://www.cybersource.com/anz)