# A review of the key Payment Technologies to be adopted by retailers and merchant intermediaries in order to enhance security and prevent fraud

*Mark McMurtrie, Director, Payments Consultancy Ltd*

## Background

Over the last 25 years we have seen a constant stream of new technologies being introduced as consumer retail payments transition from physical formats to electronic, digital and mobile payment options. One of the main drivers has been to ensure payments can continue to be made safely and prevent criminals from conducting fraud.

Card payments have traditionally relied on the use of 16 digit numbers (printed, encoded or stored within a chip, on the plastic card) to identify the payer and enable successful electronic funds transfer. If this number and the associated expiry date and 3 digit verification codes are stolen then fraud can be committed. In an increasingly digital age criminals quickly understood the value of the humble 16-digit card number and have been exploiting this at an alarming rate. Data breaches have seen large numbers of card details being harvested by fraudsters and extensive fraud being committed. The US and UK markets have seen the largest number of major data breaches. With a data breach all parties in the payments value suffer and technical solutions were needed.

Various technologies have over the years been developed to help facilitate payments and control fraud. Often multiple need to be adopted simultaneously, as there is no 'single silver bullet'. This article reviews three of the most important new payment fraud prevention technologies: Tokenisation, Point-Point Encryption and 3-DSecure 2.0. All of which have global applicability.

## Tokenisation

Tokenisation technology targets this crime in order to prevent escalating financial losses and aims to re-establish consumer and merchant confidence. This is achieved by shifting the identification of the consumer and payment account details from the actual card number to a new and different 16-digit number, which is known as a token. If the token is compromised fraud cannot be committed, as the token has no intrinsic value and cannot be used to transfer any funds. A helpful analogy is the use of poker chips instead of real cash at a casino table. The plastic casino chip cannot be spent elsewhere.

Payment Tokens are widely being introduced and are making life harder for criminals. The two main initial use cases are to secure eCommerce payments from web stores and for NFC based mobile payment options. With Apple Pay, Google Pay and Samsung Pay tokens are stored on mobile phones, providing an electronic link between the consumer, phone and payment credentials. No actual payment card numbers are stored on the mobile phone. So if a mobile is lost,

stolen or compromised fraudulent transactions can be prevented. Customers returning to an online store are identified by their associated token, allowing previous purchasing history and payment methods to be retrieved. The use of tokens also helps simplify the checkout experience.

Tokens are issued and securely managed by a variety of organisations which include the international payment networks such as Visa and Mastercard, payment services providers (PSPs) and gateways, dedicated token managers or directly by large merchants. If tokens are issued as 16-digit numbers and with format preservation then these can be processed without any changes being needed to any payment system.

**Point-to-Point Encryption**

All merchants are required to be compliant with the Payment Card Industry Data Security Standards (PCI-DSS). These cover the storing, processing and transmission of payment card details. As highlighted earlier, in recent years criminals have been stealing large numbers of sensitive card details through data breaches. In order to prevent this happening the industry has developed point-to-point encryption (P2PE) technology. This is particularly appropriate for merchants with estates of physical outlets.

P2PE ensures card details are securely encrypted immediately at the time of the purchase transaction. They are only decrypted at the central processing end point, which is typically a payment gateway or merchant acquirer. Card numbers are no longer held or stored by the merchant in the clear removing the risk of compromise, theft, financial losses and subsequent reputational damage.

The encryption takes place within a secure PIN pad that is compliant with the PCI PTS standards and running an appropriate Secure Reading and Exchange of Data (SRED) software. If P2PE is implemented in conformance with all PCI requirements and using authorised applications and components then a merchant can effectively remove their store estate from PCI DSS scope. This offers the potential for compliance cost and time savings as well as enhanced security protection. P2PE solutions have to follow an agreed Implementation Plan and operate throughout the full lifecycle of the devices.

**3-DSecure 2.0**

The 3-DSecure technology aims to improve the process of authentication of cardholders when goods or services are being purchased electronically online from computers, laptops or mobile phones. It stops payment credentials being used illegally by fraudsters. The first version of this technology was developed by Visa back in 2001 and was subsequently followed by other international payment networks who marketed it under their proprietary Verified by Visa, Mastercard SecureCode, J/Secure, SafeKey and ProtectBuy brand names. 3DSecure has successfully prevented large amounts of fraud from being committed and provided merchants who adopted it with liability protection.

However, the technology has not been adopted everywhere, been seen to increase basket abandonment rates and often been poorly implemented and communicated. Many merchants and intermediaries have a mixed view and are not advocates.

Under the auspices of EMVCo the 6 international payment brands have created a second generation of the standard, which is now available in 2018. This is a major overall and directly addresses multiple previous areas of concern. It has been designed to provide an increasingly frictionless cardholder payments experience. This will continue to be marketed by Visa as Verified by Visa but by Mastercard under the new brand name of Mastercard Identity Check. 3-DSecure 2.0 has been created for today's mobile world, wallets and apps. Static passwords have been replaced and biometrics introduced. Another significant enhancement is the increase in data points used for authentication allowing improved risk based decisions by issuers. The annoying instances of requests to sign-up within a purchase have been removed. All of these changes should deliver a significantly improved user experience.

As part of the European PSD2 legislation that came into force in 2018 and the associated Regulatory Technical Standards (RTS) there is a requirement that Strong Customer Authentication (SCA) must be implemented by a 14th September 2019 deadline. This requires the use of multi factor authentication. 3DSecure 2.0 will be able to help merchants achieve compliance. Many European merchants are currently unaware of this legal requirement (it is not just a card scheme mandate) and are yet to kick off a project. With less than 12 months to go fast action will need to be taken.

**Merchants who have not already reviewed Tokenisation, Point-to-Point Encryption and 3-DSecure 2.0 are encouraged to do so and plan for their implementation. They can deliver significant benefits, prevent fraud and reduce business risk.**

***About Payments Consultancy Ltd***

*We offer independent advice to retailers, merchant intermediaries, acquirers, payment technology companies, networks and investors. Our advisory services include strategy development, technology reviews, supplier selection and due diligence. More details can be found at www.payments-consultancy.com*