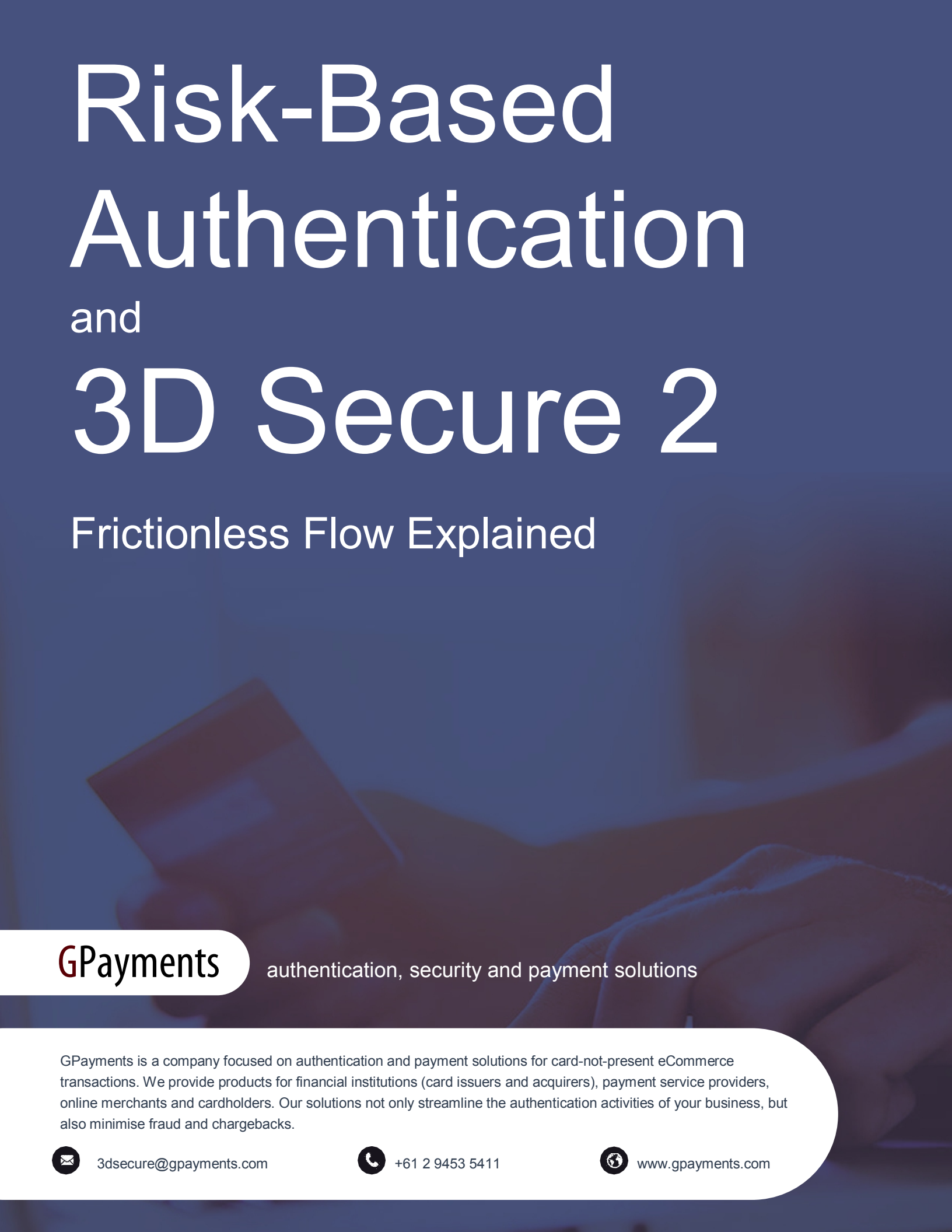
Risk-Based Authentication and 3D Secure 2

Frictionless Flow Explained



GPayments authentication, security and payment solutions

GPayments is a company focused on authentication and payment solutions for card-not-present eCommerce transactions. We provide products for financial institutions (card issuers and acquirers), payment service providers, online merchants and cardholders. Our solutions not only streamline the authentication activities of your business, but also minimise fraud and chargebacks.

3dsecure@gpayments.com +61 2 9453 5411 www.gpayments.com

CONTENTS

BACKGROUND TO 3D SECURE 2

By 2017, 50% of merchants were currently using or planning to implement 3D Secure as a fraud detection tool. In a survey of U.S. and Canadian businesses, 40% of merchants identified 3D Secure as being one of their three most effective tools against fraud (CyberSource).

The uptake of 3D Secure 1, however, was limited by a number of factors.

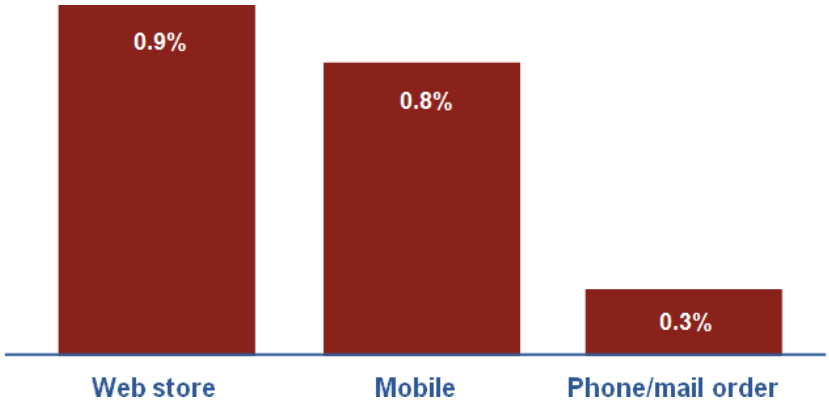
The extra steps in the authentication of cardholders during the payment process resulted in a marked increase in shopping cart abandonment.

As criminals moved to committing more fraud online and found ways to steal cardholder information and use it to make fully authenticated purchases at 3DS enabled merchant sites, the effectiveness of 3D Secure 1 was questioned.

As the habits of online shoppers have rapidly evolved over the last decade and as mobile devices have became more prevalent, the increase in mobile commerce has also brought an increase in mCommerce fraud, which is almost equivalent to the levels seen in eCommerce.

Overall Fraud Loss by Order Channel

Reported average annual fraud loss (Expressed as percent of annual eCommerce revenue)



(CyberSource)

The new EMV® 3D Secure protocol, or 3D Secure 2 (3DS2), released by EMVCo is designed to address a number of key limitations of the previous protocol and cement the technology's reputation as one of the most resilient solutions in the fight against card-not-present (CNP) online fraud.

These key changes include:

1. More robust security, to combat the ever-increasing threat of fraudulent online transactions by utilising strong customer authentication measures such as biometric and token-based authentication, instead of static passwords.

2. Compatibility with mobile devices, in line with the growing trend of mCommerce, including in-app authentication.

3. Use of risk-based authentication, supported by the collection and analysis of additional contextual data related to the purchase

4. An improved user experience, to reduce shopping cart abandonment, through frictionless flow.

The importance of frictionless flow, supported by risk-based authentication, is paramount because it will empower merchants to move even closer to a frictionless checkout experience for the customer, without compromising on the strong security that the 3DS protocol provides.

A BRIEF INTRODUCTION TO FRICTIONLESS FLOW

Frictionless flow is new to 3DS 2 and uses a process called risk-based authentication to determine whether or not a customer should be challenged for further cardholder authentication during the checkout process.

With the aim of making the customer checkout experience as frictionless as possible, if no further cardholder interaction is required, authentication is deemed to have been achieved and the transaction can proceed without requiring additional customer verification.

However, if the risk associated with the transaction is not sufficiently low enough, authentication will move onto the challenge flow. Users of 3DS 1 will be familiar with this step.

Authentication measures in the challenge flow have also been updated with the new specification to move away from static passwords. Users will now be able to use advanced measures such as biometric and token-based authentication for increased security.

HOW RISK-BASED AUTHENTICATION FACILITATES FRICTIONLESS FLOW

With the original 3D Secure protocol, customers using enrolled cards in online purchases are always challenged with an additional authentication step through an unfamiliar popup window or inline frame.

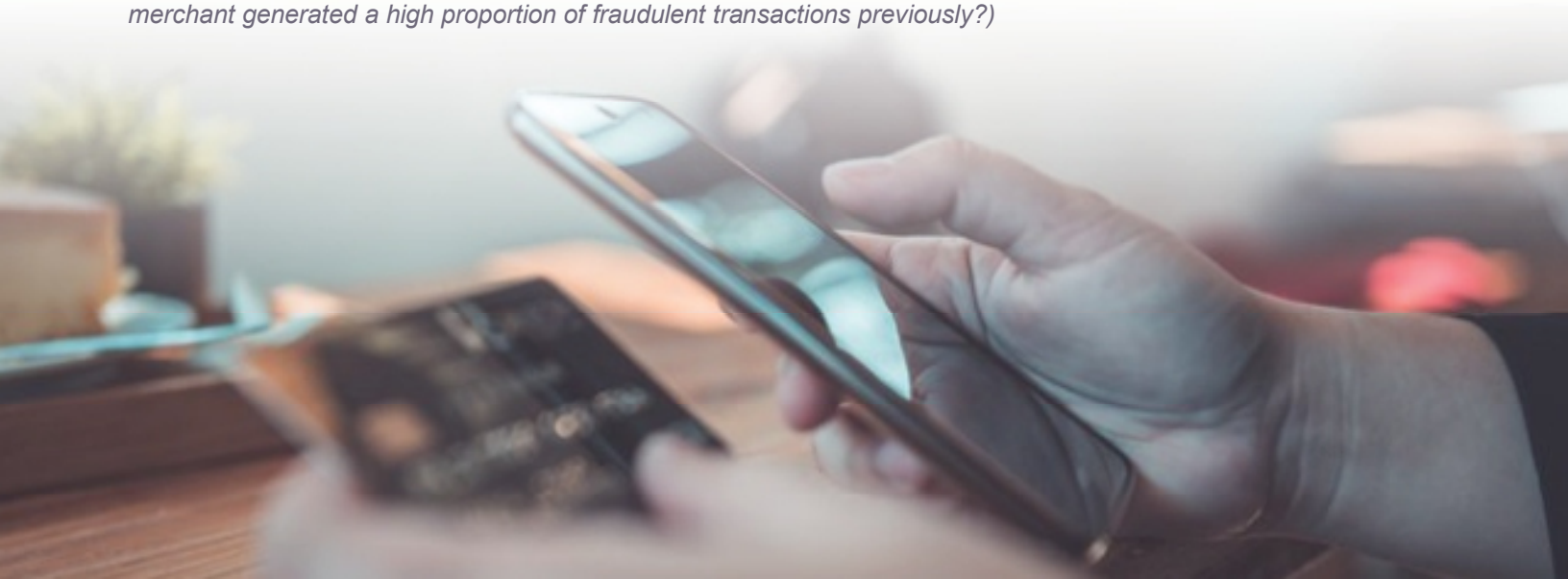
This foreign window will then request a static password, which the user has registered at some point in the past, for proof of authentication.

The additional step adds friction to the customer experience and many merchants believe that it causes an increase in shopping cart abandonment rates as a direct result.

With 3DS 2, risk-based authentication allows issuers to authenticate the cardholder without them even knowing that an authentication step actually took place.

Visa reported, in a recent study on this type of risk-based authentication, that the cardholder's checkout and payment transaction time is reduced by 85% and cart abandonment rates decline by up to 70%. Visa estimates that, with 3DS2, 95% of transactions will be low risk, requiring no additional customer verification and typically, less than 5% of transactions will require additional customer verification. Even Mastercard's more cautious estimate predicts approximately 80% of transactions would be categorised as low risk and fully authenticated, 15-18% would be medium risk requiring further authentication and less than 2% would be high risk and automatically fail authentication.

The risk-based authentication that provides this frictionless flow is dependent upon additional data captured during the checkout process and transaction history data held by both issuers and merchants. Additional data can include behavioural checks (*has the cardholder purchased online for this merchant previously?*), device checks (*where is this device located? has the cardholder used it for online purchases previously?*), and merchant checks (*has this merchant generated a high proportion of fraudulent transactions previously?)*



As part of the 3DS2 process, merchants capture a rich data set of information from the customer during the checkout process. This data is collected from either the browser or mobile device being used in the CNP transaction.

The merchant can then share this information with the card issuer.

In turn, the issuer will analyse the information provided to assign a level of risk, based on the specifics of the transaction.

This will allow the issuer to make an informed decision as to whether or not an additional authentication step is necessary.

If the risk is below a certain threshold, the issuer will approve the cardholder authentication without the need for an additional challenge and customers will not even know that authentication has taken place. If the risk is above the threshold, the transaction will move into the challenge flow and the cardholder will be required to be further authenticated.

As a result, merchants can expect a significant reduction in cart abandonment due to the implementation of 3DS2.

Merchants will also enjoy protection through liability shift, where the liability for fraudulent chargebacks typically shifts to the issuing bank. This benefit is unique to the 3D Secure protocol and not provided by any other rule-based application.

HOW AND WHAT TYPE OF INFORMATION IS CAPTURED

Customers will interact with merchants in CNP transactions via a browser and/or a device. The type of information and how it is being captured will depend on this method of interaction. The information can essentially be broken down into three types, device information, browser information and merchant risk information.

Device information

Device information is collected through mobile SDK's. If a merchant has a mobile app with 3DS2 integration, the 3DS SDK will capture the necessary information directly from the device that the customer is using to process the transaction and then send it to the issuer for risk-based authentication analysis. There are four categories of app-based information:

Common device information - consists of 12 data elements, which are common to all mobile platforms. Information captured includes what type of platform is being used together with the specific IP address. Device specific information is also captured, such as device name, device model, even the screen resolution. Device software such as operating system together with OS version is also included. Finally, more abstract information such as the time zone and position of the device is also captured.

iOS specific information - includes an additional 13 data elements on top of the 12 elements captured as part of the common device information. This applies specifically to Apple devices and includes elements such as system and label font size, preferred language and default time zone.

Android specific information - includes an additional 136 data elements on top of the common device information. These elements range from the very detailed, such as the date format and screen brightness, to more high-level data, such as device ID, network and SIM operator name, device manufacturer and serial number.

A complete list of the device information collected by the 3DS SDK is available in the EMV® 3-D Secure SDK—Device Information specification, available on EMVCo's website.

Browser information

If transactions are conducted on the merchant's website through a browser, data is captured by the 3D Secure Server in the merchant domain and then sent on to the issuer for risk-based authentication, similar to the device information flow.

This detailed information captured from the customer's browser will in some instances be similar to the device information collected above and includes the following 9 elements:

Accept Headers

Indicates which content (MIME) types the browser is able to understand.

IP Address

The IP address of the PC on which the browser is running.

Java Enabled

Indicates if the browser is Java enabled

Language

Indicates which language the cardholder's browser is using.

Screen Colour Depth

Indicates the bit depth of the colour palette used for displaying images on the screen.

Screen Height

Indicates the total height of the cardholder's screen in pixels.

Screen Width

Indicates the total width of the cardholder's screen in pixels.

Time Zone

Indicates the time difference between UTC and the cardholder's local time.

User-Agent

Indicates the exact content of the HTTP user-agent header.

Merchant risk information

The issuer might also collect and utilise additional cardholder information to help improve the accuracy of the risk-based authentication.

For both browser and app scenarios, supplementary cardholder account and transaction information can be provided by the merchant to the issuer.

This additional data is NOT mandatory but it is strongly recommended that this information is made available to improve the accuracy of the issuer's risk-based information and thereby reduce the number of cardholder challenges through the challenge flow.

There are 4 sub-categories of merchant risk information.

Cardholder account information customer data held by the merchant as part of a registered account. This includes basic information such as account age, date of any changes made to the account, shipping address and frequency of transactions, including both successful and abandoned transactions.

Specific purchase information relates to the purchase habits of the customer, whether the products or services being purchased have been ordered before (reorder items indicator), location the order is being shipped to (shipping indicator) and was it pre-purchased (pre-order purchase indicator).

Prior transaction authentication information shows data on past transaction authentication, whether it was frictionless or whether the cardholder was challenged for additional authentication. Additional information could include date and time of previous authentication attempts.

The merchant cardholder account authentication information relates to the actual relates to the actual customer login to the merchant account and whether it was via a browser or a mobile application. Optional information provided here would include issuer credentials and third-party authentication, for example Google. If existing information is not available on the cardholder, the data will be set to guest.

CONCLUSION

The growth in the complexity and frequency of CNP fraud has forced merchants and card issuers alike to apply more stringent security measures in order to verify the true identity of cardholders in CNP transactions.

Increased security, however, often comes at the expense of the customer experience and balancing an enjoyable customer experience with powerful risk management processes will always be an ongoing challenge.

Frictionless flow, which is dependent upon risk-based authentication, is what truly sets the new and improved 3DS2 protocol apart from other authentication engines. It strikes the perfect balance between unwavering cardholder security, while still providing the customer with a smooth checkout experience.

At its core sits rich-data capturing capabilities, which enable merchants and issuers to collect and share more quality information on which risk can be assessed and authentication decisions based. The end result is accurate and intelligent risk-based decisions where as much as 95% of transactions are frictionless requiring no further customer interaction for authentication.

The 3DS2 technology provides flexibility to online merchants enabling them to implement the protocol in the two very different ecosystems of app-based and browser-based payments.

Everyone's a winner with 3DS2. Customers receive greater protection against fraudulent transactions with an improved user experience, and issuers can more accurately authenticate cardholders with increased rich-data capturing and sharing capabilities.

Finally, merchants can enjoy reduced cart abandonment while benefiting from a potential liability shift in fraudulent chargebacks. Ultimately, merchants can leverage the benefits of incorporating the 3DS2 protocol into their shopping platforms and providing customers with greater peace of mind through a robust transaction security application.

For further information, please contact 3dsecure@gpayments.com