GPayments

# FRICTIONLESS FLOW

## WITH 3D SECURE 2.0

WWW.GPAYMENTS.COM

AUTHENTICATION | SECURITY | PAYMENT SOLUTION

# CONTENTS

# BACKGROUND

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.

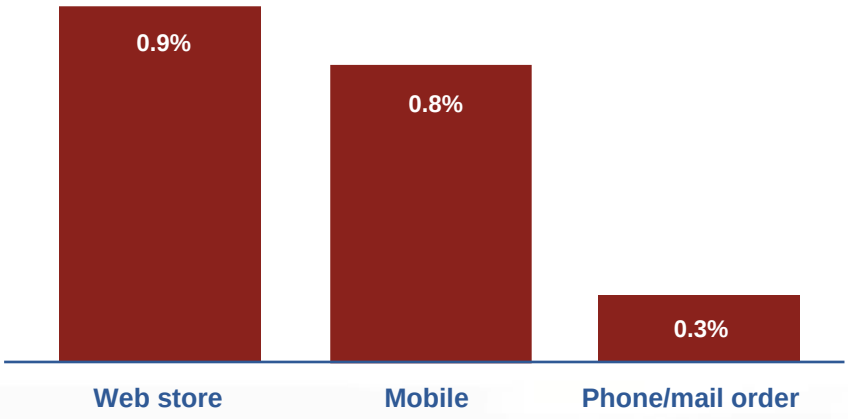
As criminals moved to committing more fraud online and found ways to steal cardholder information and use it to make fully authenticated purchases at 3DS enabled merchant sites, the effectiveness of 3D Secure 1 was questioned.

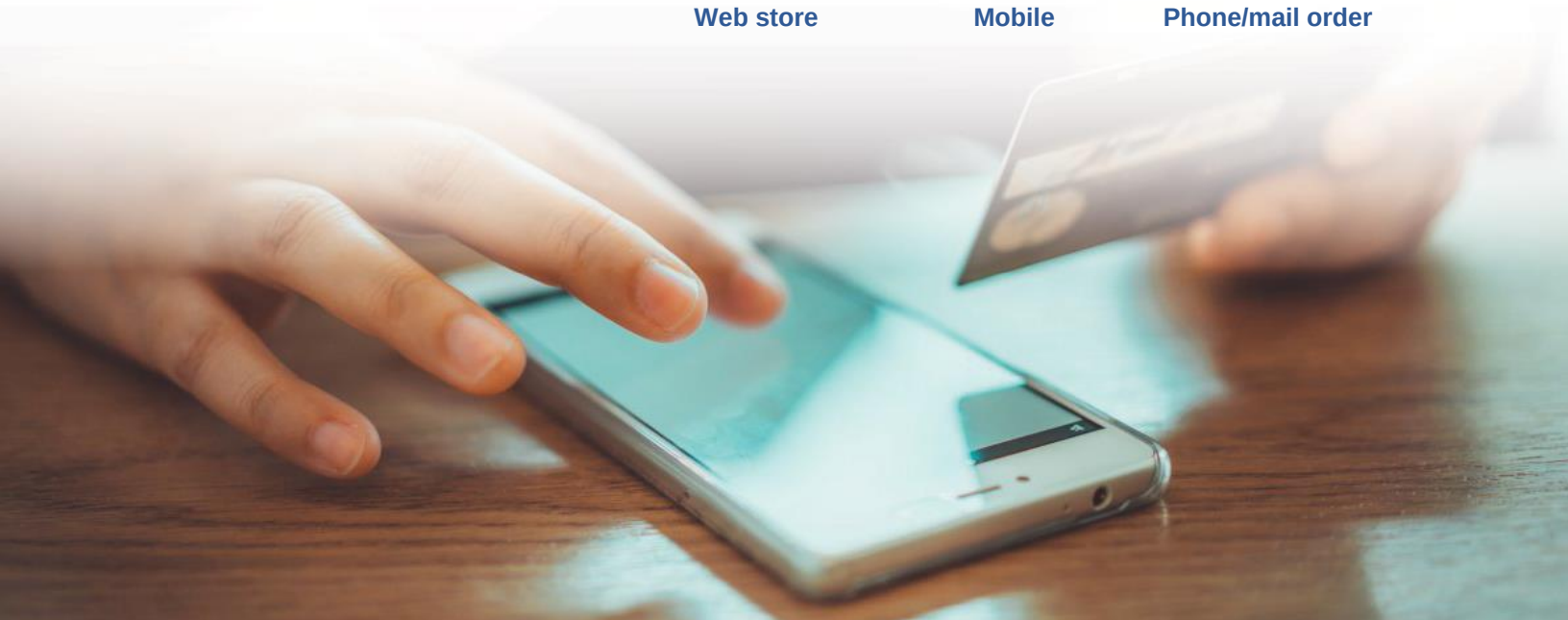
As the habits of online shoppers have rapidly evolved over the last decade and as mobile devices have became more prevalent, the increase in mobile commerce has also brought an increase in mCommerce fraud, which is almost equivalent to the levels seen in eCommerce.

Frictionless flow is important because it will empower merchants to move even closer to a frictionless check-out experience for the customer, without compromising on the strong security that the 3DS protocol provides.

## Overall Fraud Loss by Order Channel

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



(CyberSource)

Thenew EMV® 3D Secure protocol, or 3D Secure 2 (3DS2), released by EMVCo is designed to address a number of key aspects 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 INTO FRICTIONLESS FLOWS

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 DOES RISK-BASED AUTHENTICATION WORK WITHIN THE 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 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 [https://globalrisk.mastercard.com/wp-content/uploads/2015/12/Advantages-of-Risk-Based-Authentication.pdf] more cautious estimate predicts approximately 80 percent 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 it 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.

# EXACTLY HOW AND WHAT TYPE OF INFORMATION IS CAPTURED?

There are two main channels in which customers will interact with merchants in CNP transactions. The type of information and how it is being captured will depend on this method of interaction. As a result, information can essentially be broken down into three different types.

## Device information

The first is 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 ACS for risk-based authentication analysis.

This information will be app-based and can be further broken down into four categories:

**The common device information** consists of 12 data elements which are shared on all mobile platforms. Information captured will include what type of platform is being used together with the specific IP address. Device specific information will also be captured like 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** will include an additional 13 data elements on top of the 12 elements captured as part of the common device information. This will relate specifically to Apple devices and include elements such as system and label font size, preferred language and default time zone.

**Android specific information** will include an additional 136 data elements on top of the twelve elements captured as part of the common device information. These elements will 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.

**Windows 10 mobile specific information** will include an additional 25 data elements on top of the twelve elements captured as part of the common device information. This will include publisher host ID, resolution scale, system product name and system manufacturer.

For a full list of information parameters collected by the 3DS SDK, the EMV 3-D Secure SDK—Device Information specification can be consulted.

## 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 ACS for risk-based authentication, similar to the device information flow.

This accurate browser information captured from the customer browser will in some instances be similar to the device information collected above and include the following 9 elements:

### Accept Headers

The Accept header tells the server what file formats, or more correctly MIME-types, the browser is looking for. Let's take a look at Firefox's Accept header


### IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.


### Java Enabled

Java is a programming language that produces software for multiple platforms.

### Language

language is a formal language that specifies a set of instructions that can be used to produce various kinds of output.

### Screen Color Depth

The number of bits used to hold a screen pixel. Also called "pixel depth" and "bit depth," the color depth is the maximum number of colors that can be displayed.

### Screen Height

JThe height above the ground of an imaginary screen that the aircraft would just clear when taking off or landing, in an unbanked attitude and with the landing gear extended.

### Screen Width

The size of a screen is usually described by the length of its diagonal, which is the distance between opposite corners, usually in inches.

### Time Zone

The term time zone can be used to describe several different things, but mostly it refers to the local time of a region or a country.

### User-Agent

user agent is software (a software agent) that is acting on behalf of a user. One common use of the term refers to a web browser telling a website information about the browser and operating system.

## 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 3DS 2. 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 3DS 2 protocol into their shopping platforms andproviding customers with greater peace of mind through a robust transaction security application.