

3DS 2.0

A STEPPED-UP APPROACH TO PAYMENT AUTHENTICATION



3DS 2.0: A Stepped-Up Approach to Payment Authentication

Poorly designed authentication experiences have an adverse impact on customer engagement, fraud mitigation, and operational efficiency. The paper details how 3D Secure 2.0 can help issuers and merchants achieve the right balance between convenience and security.



Evolving E-Commerce Landscape and Fraud

In 2018 one out of every ten dollars spent globally occurred over a digital channel. Digital convergence, the IoT revolution and proliferation of transactional channels and instruments is fueling growth of online marketplaces. Additionally, the banking world is becoming more open; paving the way for new entrants and further expansion.

With a significant bulk of interactions between consumers and merchants shifting online, fraud threats have accelerated equally rapidly. There has been an intensification in the sophistication and velocity of fraud attacks over these channels. In a recent report Javelin Research estimated card not present (CNP) fraud is now 81% more likely than point of sale fraud and represents 7% of total retail losses. Likewise, in Europe CNP fraud accounts for 73% of the total card fraud, with total losses pegged at €1.31B in 2016 by the EBA.

Limitations of 3D Secure 1.0

Identity, security, and trust are fundamental to commerce. For payment service providers reliable authentication and anti-fraud counter-measures are central to maintain the growth momentum. Merchants and card issuers have deployed 3DS 1.0 to provide an additional layer of defense against fraud threats. Commercially (3DS) offers significant benefits. The service uses real-time authentication to lower fraud by replicating the level of security of a card-present transaction for remote transactions. This instills confidence in consumers and offers an established recourse process for disputed transactions. Merchants also benefit from a liability shift towards the card issuer, reducing chargebacks to the merchant alongside lower cost per transaction.



Yet, in several countries adoption has lagged. One of the biggest challenges in the fraud detection space is the consumers' expectation of immediacy. A transaction needs to be fulfilled in the blink of an eye, and therefore, fraud controls should be transparent to the consumer. To use 3DS, customers, however, need to complete a one-time enrollment process with their issuing bank. On entering card details, customers are redirected to another page, where the issuer requests for a passcode to authenticate the purchase. This step combined with confusing web redirect experiences impacts fast-lane checkout, erodes the customer experience and discourages use among merchants.

In the USA adoption rates among merchants are as low as 5% due to unfriendly customer experience and high rates of basket abandonment. In Europe, where the 3DS protocol is widely adopted by issuers, an approximate 50% of account holders are enrolled, and only 25% of eCommerce transactions are verified. Only two-third of the top 100 merchants in the UK are using Secure Code; in Germany, it's even less at one-third³.

3DS 1.0 is, furthermore, potentially vulnerable to phishing and "man in the middle" attacks. This is caused by the redirection to another URL for the 3DS process. Fraudsters can generate a similar looking pop-up window to steal personal credentials.

The protocol also lacks support for native in-app purchases, a significant drawback in a rapidly-growing mobile economy.



A New Approach: Balancing Risk and User Experience

The development of 3DS 2.0 addresses the inherent limitations in the previous version of the protocol to fit current needs of merchants and consumers. Specifically designed to balance the demand for a single click checkout experience with the requirements for secure payments, the new standard brings a range of improvements. This includes:

- Frictionless Authentication
- Adaptive Risk-Aware Approach
- Support for Mobile and IoT Commerce
- Merchant Opt-Out



Comparison between 3DS 1.0 and 3DS 2.0

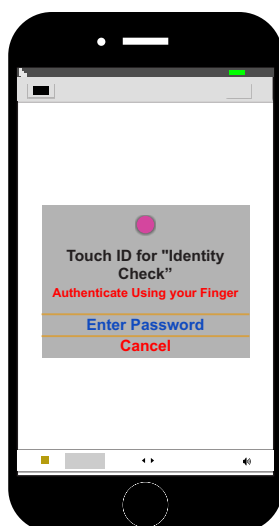
Requirement	3-D Secure 1.0	3-D Secure 2.0
Frictionless Flow	Absent (Every online purchase transaction must go through an authentication process)	Cardholder interaction is not required for all online transactions
Customer Enrollment	Enrollment required	Eliminates enrollment
Authentication Methods	Static passwords	Sophisticated authentication such as biometrics and token-based authentication
Risk Decisioning	No risk-based decisioning	Risk based decisioning based on certain parameters to authenticate customers (device, transactional and merchant parameters)
Form Factors	Browser-enabled	Cross-channel, device-agnostic support. Supports digital wallets, in app purchases, IOT devices
Use Cases	Payment use cases	Additional use cases - Enables non-payment customer authentication that allows services like Identification and Verification (ID&V) for mobile wallets and secure request of tokens for card on file

Frictionless Authentication

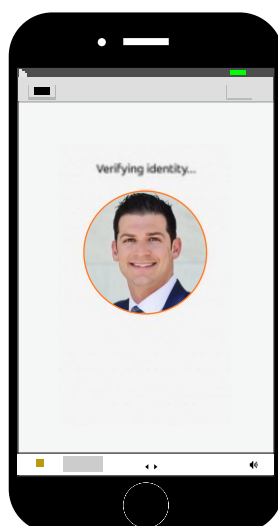
Customer experience is central to the new protocol, as it eliminates onerous features that slow transactions, including pop-up windows that require consumers to enroll and input information. 3DS 2.0 exploits richer cardholder and device data exchanged between the merchant and the issuer to assess whether a cardholder should be allowed or challenged for further verification.

Considering passwords can be easily forgotten and compromised, 3DS 2.0 further streamlines the transaction process by removing reliance on static passwords and knowledge-based questions to verify the authenticity of the cardholder in the challenge flow. The new protocol employs biometric and out-of-band authentication mechanisms, as a second-factor authentication trigger to encourage cardholders to make purchases using their preferred medium without compromising on security.

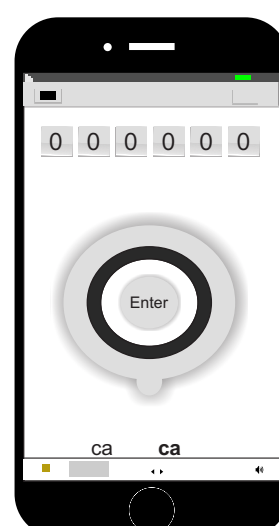
Range of Authentication Methods



Touch ID



Selfie pay



Mobile OTP

Adaptive Risk-Aware Approach

At the core of 3DS 2.0 is dynamic risk-based authentication, enabling merchants deliver customer-centric, frictionless transaction experiences. The risk-aware authentication approach exploits powerful machine learning technology and data science to continually learn fraud patterns and fine-tune authentication decisioning, as fraud threats evolve and mutate. Risk-based authentication can run transparently in the background, without interrupting the user experience, and offers multiple step-up authentication methods for suspect transactions.

EMVCo's new protocol exploits rich data exchanged in the authentication request between the merchant and the issuer to identify potentially risky transactions. More than 150 data elements are exchanged between cardholder, merchant, and the issuer, and the contextual data shared exceeds the earlier version by 10X. A range of variables are leveraged to classify the risk quotient per transaction and make authentication decisions.



80%-95%



Users are good

Let them in with a great user experience

10%-15%



Users are suspected as rogue

Subject them to a adaptive, dynamic authentication

Based on suspicion level - trigger additional authentication challenges

The data provides a wealth of intelligence and can be leveraged as a powerful predictor of fraud. By combining multiple data points, issuers can risk-score transactions, perform a range of checks to ensure the customer is legitimate and accurately flag fraudulent transactions. Based on contextual data, if the risk is below a defined threshold, issuers can approve transactions without subjecting them to additional authentication.

Data Sources



Transaction Information

- ✦ Repeated transactions in a short span
 - ✦ Implausible travel velocity (e.g., transactions originating from two separate geographic or merchant locations within a short span)
 - ✦ Deviation from normative transactional patterns – example higher and amount, volume, different merchant location or device, country or odd shopping hours
 - ✦ Transaction currency
 - ✦ Address verification checks mismatch between shipping and billing address
 - ✦ Mismatch between shipping and invoicing address
 - ✦ Different customers with different shipping addresses, but with the same zip code.
 - ✦ Recurrent transaction and last
 - ✦ First purchase at a merchant location
-



Merchant Information

- ✦ Transactions originating from merchant categories deemed risky
 - ✦ Higher velocity and volume of transactions than permissible
 - ✦ High volume of chargebacks and transaction declines
 - ✦ Merchant risk score
 - ✦ Age of merchant on the network
 - ✦ Merchant country to protect against country-specific risks
 - ✦ Acquirer BIN
 - ✦ Acquirer merchant ID
-



Cardholder Information

- ✦ Basic card information such as account number, card BIN, cardholder name, card expiry date to verify customers
 - ✦ Account usage patterns
 - ✦ Data on past transaction authentication, whether it was frictionless or whether the cardholder was challenged for additional authentication
-

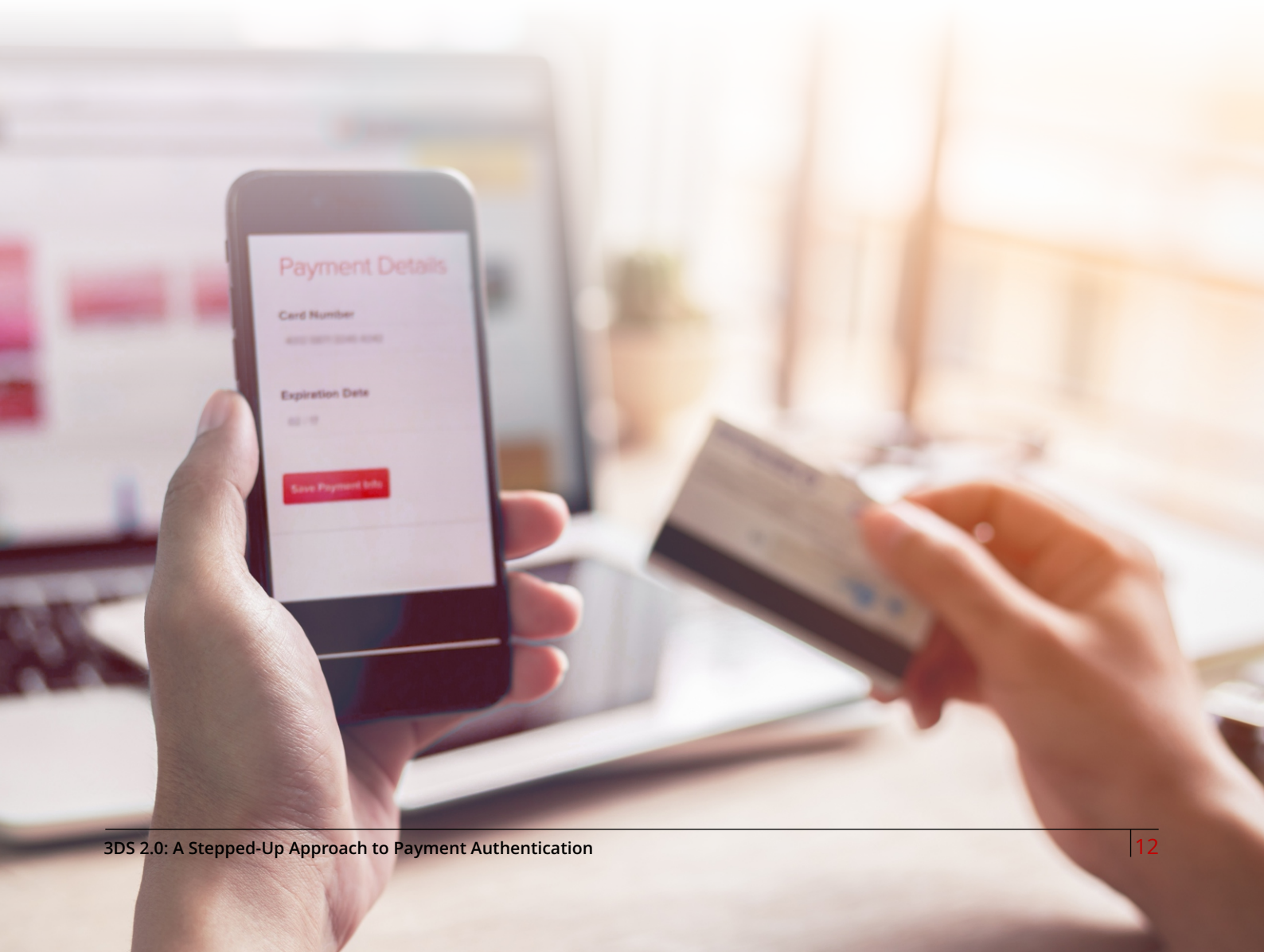


Device Information

- ✦ Type of platform being used, IP address, device model, screen resolution, device software such as operating system
- ✦ Device scheme such as network operator code, network country code, network operator name
- ✦ iOS and Android specific information - includes additional data elements on top of the basic elements captured as part of the common device information
- ✦ Browser details including browser IP, agent and location to detect originating source of the transactions

Supports Mobile and IoT Commerce

Mobile customers working on a smaller screen expect instant gratification and have less tolerance for security methods that make the checkout process inconvenient and clunky. 3DS 2.0 is capable of seamlessly integrating with mobile apps as well as browser-based environments. 3DS 2.0 extends authentication to in-app purchases and digital wallets that store card details to satisfy the demand for a seamless mobile shopping experience.



Merchant Opt-Out

3DS 2.0 provides merchants the flexibility to use individual decisioning to enforce or skip 3DS on a transaction-by-transaction basis or use their own risk models to approve or deny a sale. Whilst this entails a liability shift if the purchase is fraudulent it could reduce false positives and deliver an optimized experience for trusted customers.

Promise of Authentication-As-A-Service

FSS Secure3D, a risk-based authentication payment service, uses dynamic rules to improve online transaction security and encourage the growth of e-commerce payments. FSS Risk-based Authentication-As-a-Service allows customers to harness aggregated anonymized data (risk score) to effectively control fraud and defend against fast-changing fraudster behaviors. The result is a competitive edge in customer experience with reduced false positives and low fraud levels.

FSS Secure3D is hosted on FSSNeT, FSS private cloud. For issuers and payment service providers Authentication As-a-Service enables banks to go live at a minimal upfront cost and a competitive 'pay-as-you-use' commercial model. FSS Software-As-a-Service capabilities include:

Secure Services Infrastructure: FSSNeT environment is PCIDSS 3.2 certified, assuring a high levels of security. Our comprehensive and robust security practices for application and data protection include continuous threat assessment malware protection, data encryption, security patching, policy compliance and management.

Salable, On-Demand Services and Reliability: With FSSNeT customers can seamlessly upgrade capacity in line with growth in transactions. Further processors and banks are assured of high levels of service reliability with state-of-the art AI-based tools to monitor service performance levels.

Accelerate Product Development and Innovation: Customers have immediate, seamless access to new functional innovation and upgrades with zero services disruption.

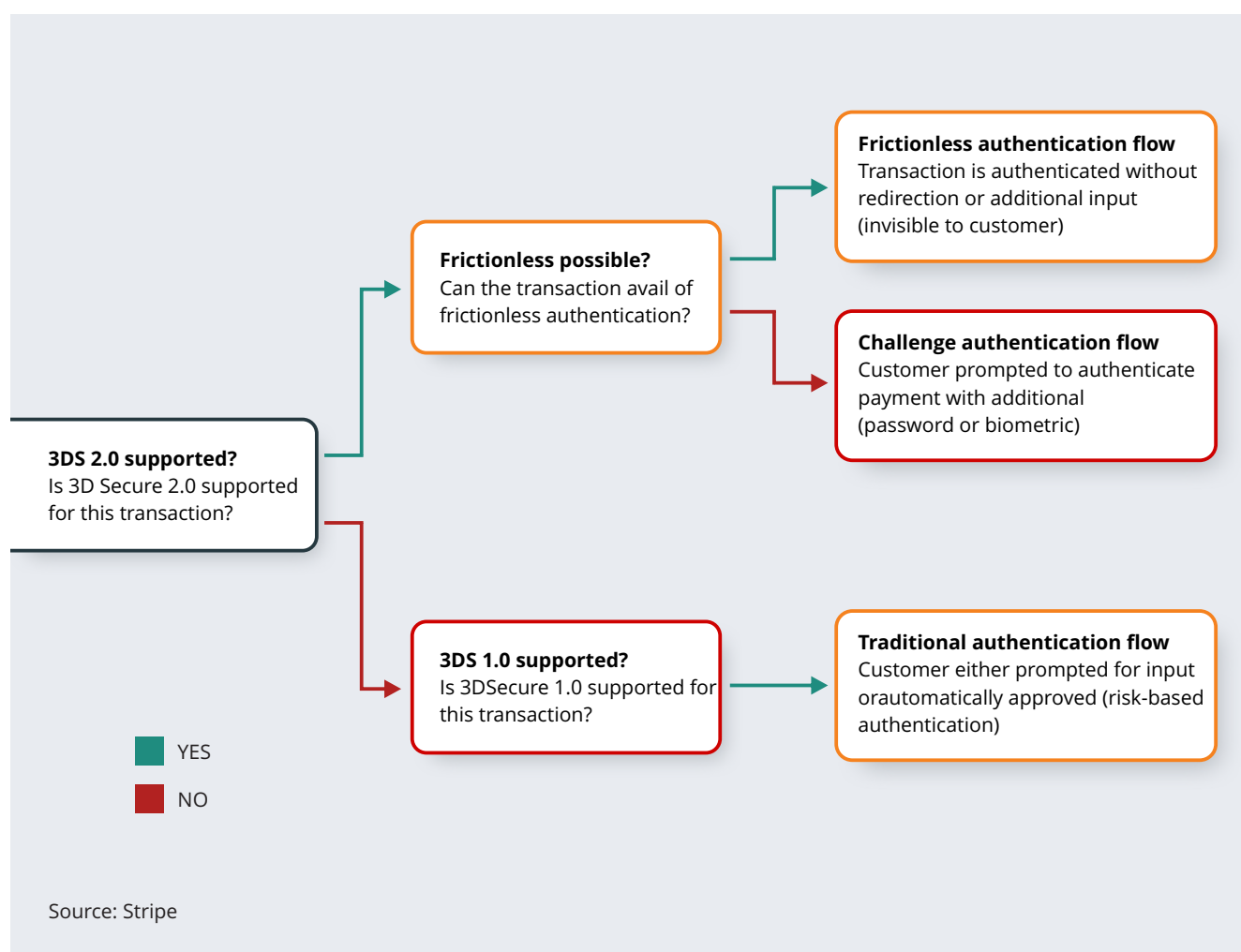
Reduce Certifications and Compliance-related Labor: FSS assumes complete responsibility for certifications from interchanges and compliance with regional regulatory mandates including SCA and PSD2.

Data Security and Reporting: FSS Secure3D is compliant with data security, maintenance and privacy norms governing each region as well as regulatory reporting requirements in event of data breaches.

Business Dashboards: Rich operational and business analytics to provide insights and ideas to improve performance.



Support for 3DS 1.0 and 2.0: FSS supports the existing 3DS 1.0 and the brand-new 2.0 protocol. During the checkout the solution automatically determines which protocol should be used to process the card. 3DS 1.0 and 3DS 2.0 will operate in parallel for some time. For customers with existing implementations, FSS extends support for both versions and domain specialists can ensure a smooth migration experience from 3DS 1.0 to 3DS 2.0, to assure a consistent customer experience.



Privacy by Design: FSS Secure3D can address the challenge of providing dynamic risk assessment while maintaining data privacy through use of anonymization and encryption techniques.

To Know More

FSS can help issuers and payment processors migrate to 3DS 2.0. Send an email to products@fsstech.com to connect to our product experts. FSS customers can contact their account representative for a detailed assessment on how we can ease migration to 3DS 2.0

www.fsstech.com

Sources

- 451 Research, Global Unified Commerce Forecast, 2018
- Juniper Research, Future Fraud – 3 Dynamics Changing Fraud in 2019
- Pymnts.com, The Perfect Secure Payments Storm
- European Central Bank: Fifth report on Card Fraud