WE ANSWER FREQUENTLY ASKED QUESTIONS RELATED TO 3DS 2.0

What are the factors contributing to the rise of CNP Fraud?

Globally card not present (CNP) fraud is on the rise, fueled by an interplay of factors – introduction of EMVCo, higher transaction flows over online channels, new open banking models and real-time payments.

Introduction of EMVCo

The adoption of EMV (Europay®, Mastercard® and Visa®) in the past few years has resulted in the migration of fraud to card not present channels. For instance, in 2017 the US alone registered an 81% increase in card not present fraud, according to research from Javelin, 2018 Identity Fraud Study.

Growing m-Commerce Transactions

Consumers are increasingly interacting with brands using mobile devices. Across geographies between 20% and 50% of all transactions originate from a mobile device or an app. Online fraud is mirroring the rapid increase in the popularity of mobile payments, expanding rapidly beyond traditional PCs to mobile and tablet devices.
Real-time Payments

Another factor is growth in real-time payment networks. Real-time payments mean everyone can move money quickly including fraudsters. For example, a year after the UK introduced the Faster Payments System in 2008, fraud rates registered 132% growth.

Open Banking

The introduction of Open Banking and Payment Services Directive2 fundamentally alter the rules of the security game. As banks implement APIs and open their infrastructure to third party payment providers under PSD2, a new range of opportunities for fraudsters is potentially created. European Union's PSD2 Regulatory Technical Standards on Strong Consumer Authentication aims to safeguard customers.

For issuers, convergence of these factors entails a shift from a compliance-centric to an effective proactive security mindset.
What are some of the real-time use cases for fraud prevention?

Issuers can use a combination of merchant, cardholder, device, location and transaction related parameters to gain a clear picture of the traits that separate legitimate transactions from fraudulent ones. Using these variables, FSS Secure3D can uncover a range of unseen fraud patterns in real-time. A select list of use cases we support is included below:

- Implausible travel velocity (e.g., a user logs into Cape Town, South Africa, within 10 minutes of the same user logging into Mumbai, India).
- The same device makes repeated attempts to log into multiple sites within a brief interval.
- Mismatch between the customer’s home and the shipping address.
- Merchant score based on business category, transaction patterns, chargeback volumes and refund amounts.
- Transactions originating from high-risk countries.
- Transactions originating from hot-listed and blacklisted cards.
- Suspicious combinations of locale settings on a computer (e.g., a browser’s locale set to the US with the OS locale set to a South Asian country and a device’s IP address physically located in South America).
How are authentication technologies evolving?

Existing solutions to authenticate customers create a rift between security and customer experience. On the one hand identity management solutions need to provide identity assurance. At the same time, they need to make it easy for service providers to deliver customer convenience. Several times these goals are at odds with each other.

In countries such as India where the second factor of authentication is mandatory – cart abandonment rates can be as high as 20%, due to latency introduced by authentication-related processes at checkout.

Increasingly, we are seeing the market move towards risk-aware authentication. Technologies like, Biometrics, AI, and machine learning are evolving to authenticate customers, secure transactions, and mitigate fraud losses. At FSS, we have responded to the increasing threat of online fraud by developing AI-based fraud detection tools and advanced multi-factor authentication techniques, involving out-of-band authentication and using biometric technology for identity verification.

Biometrics is particularly applicable for transactions originating from mobile devices, many of which are equipped with fingerprint, iris and facial recognition and can also analyse voice patterns to authenticate customers.
How does FSS Secure 3D benefit issuers. And what’s new?

The current 3D Secure protocol where transactions are authenticated using a one-time password has inherent limitations. The additional step during the checkout process results in high cart abandonment among customers. The impact is especially pronounced in mobile apps, where applying 3D Secure may redirect customers from the native app and onto a bank’s website that isn’t optimized for mobile devices.

FSS Secure3D, a secure real-time risk-based authentication solution, built on EMVCo 3DS 2.0 specifications, addresses many of the shortcomings seen in 3DS Version 1.0. FSS Secure3D deploys sophisticated machine-learning algorithms to continually learn fraud patterns and generates automatic alerts on detecting anomalous transactions. This is achieved by examining rich data streams exchanged between merchants and issuers to validate customer identity and risk-score transactions using a combination of location, merchant, transactional and device related attributes. For high risk transactions, FSS Secure3D dynamically provisions additional verification checks such as biometric-based identification or a one-time passcode. This renders 100% challenge rates obsolete, enabling issuers and merchants to strike the right balance between security and customer convenience.
Will the deployment of FSS Secure3D ensure all transactions are authenticated automatically?

To fraud score transactions in real-time, ML-based risk scoring algorithms need to be trained. In the early deployment stages, the number of transactions authenticated seamlessly, would depend on the richness of existing data available around customer transaction patterns.

Over time, with growth in transaction volumes, the system learns cardholder shopping patterns and the number of transactions subject to a second factor of authentication would be a small subset of total transactions.

Can FSS Secure3D help meet PSD2 SCA guidelines?

Yes. PSD2 requires payment service providers to ramp-up identity verification processes and mandates customer authentication using at least two elements; something they have (e.g. a phone or a hardware token), something they are (e.g. fingerprint or face recognition), and something only they know (e.g. a password or a PIN).

There are exemptions in place, that can be requested by merchants:

- Transactions under €30 (US$ 33.93) are exempt, while merchants with fraud rates between one basis point and six basis points for remote, card-based payments are also exempt.

- Subscription or recurring transactions with a fixed amount will be exempt from the second transaction onwards. Only the initial transaction will require SCA. If the amount changes, the transaction will be subject to a second factor of authentication.

- Transactions originating at merchants whitelisted by the cardholder will be exempt from the second factor of authentication.
Enabling 3DS 2.0 helps cover these SCA requirements. Modelled on EMVCo 3DS2.0, FSS Secure3D provides an industry standard approach to comply with the new European Union’s PSD2 Regulatory Technical Standards on Strong Consumer Authentication that take effect in September 2019.

**Is FSSSecure3D certified by EMVCo?**

Yes. FSS is an EMVCo member and is amongst the first set of digital security solution providers to be EMVCo certified. FSSSecure3D is approved by major card interchange schemes including Visa and MasterCard and is currently undergoing Amex certification.

**How do customers migrate from 3DS 1.0 to 3DS 2.0?**

FSS supports EMVCo 3DS 1.0 and the 3DS 2.0 protocols. For customers with existing solutions, FSS with experience of successful large-scale migration projects, can ensure seamless transition from 3DS1.0 with minimal associated overheads.
Why FSS for Secure3D?
What value does FSS bring to the table?

Enhanced Authentication
At the heart of FSS Secure3D is our risk-based authentication engine. We have adapted a clear box approach and built accurate data models that interpret and learn from the results and assess complex scenarios for improved risk decisioning.

Supports Hosted Services Model
Further, FSS offers the solution on FSSNeT, FSS private cloud. This helps us in leveraging data elements across our participating client base in order to provide a positive or a negative customer index. Issuers can potentially benefit from collective intelligence and can make better informed fraud decisions.

Deep Domain Expertise
Unlike many providers in the market, FSS has over 28 years of experience in deploying integrated payment solutions for leading Tier One Banks and payment processors globally. FSS has extensive experience in Issuance, Acquiring, Big Data Analytics and Digital Security, which enables us to understand issuer and merchant payment technology environments and deploy the right authentication solutions.

Proven Player
We have a proven implementation track record. Currently FSS Secure3D V1.0 is deployed by 20+ issuers and acquirers across Middle East, Europe and South Asia and we process over 100M transactions annually.
About FSS

Financial Software and Systems (FSS) is a leader in payments technology and transaction processing. The company offers an integrated portfolio of software products, hosted payment services and software solutions built over 27+ years of experience. FSS, end-to-end payments products suite, powers retail delivery channels including ATM, POS, Internet and Mobile as well as critical back-end functions including cards management, reconciliation, settlement, merchant management and device monitoring. Headquartered in Chennai, India, FSS services leading global banks, financial institutions, processors, central regulators and governments across North America, Europe, Middle East, Africa and APAC and has 2,500 experts on-board. To know more, write to products@fsstech.com