LexisNexis®
RISK SOLUTIONS

WHITE PAPER

Using LexisNexis® Risk Solutions to enhance risk decisions in the 3-D Secure customer journey

More customers rely on online transactions than ever before

Digital commerce is one of the key driving forces behind the growth of global economies, providing access to goods and services to online consumers wherever and whenever they choose. While this facilitates inclusion on a global scale, it also presents challenges for merchants, issuers and acquirers, to verify identities and authenticate transactions without introducing friction into a competitive online marketplace.

A poorly timed step-up or overly aggressive authentication strategy risks pushing both loyal and occasional consumers to the next available online retailer. However, without robust security protocols, businesses can expose themselves to unmanageable fraud rates

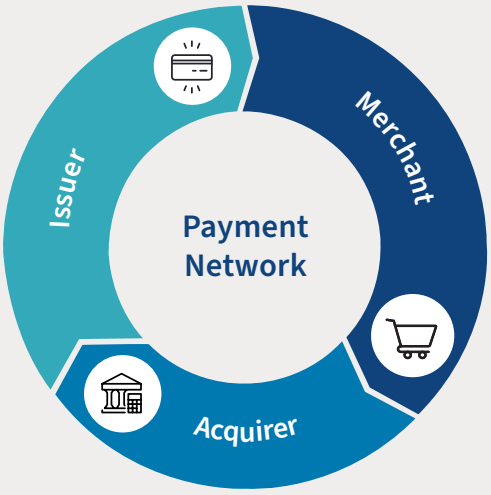
The symbiotic balance between effective and low friction fraud control, with the ability to reliably distinguish good customers from potential fraudsters across the online journey, is a key imperative for business growth.

Introducing digital identity intelligence into the 3-D Secure (3DS) authentication protocol

The 3DS protocol provides a secure framework to link the acquirer with the issuer in order to authenticate a cardholder during an e-commerce transaction. It was updated in 2018 to include a mobile component and to further streamline the customer experience without compromising security.

3DS 2.x Benefits

- A low-friction authentication process
- Mobile friendly specifications that integrate with both mobile browsers and mobile apps
- The ability for merchants to share 150 data points with issuers, as opposed to 15 in the original protocol
- A flexible opt-out policy



With the expanded scope of 3DS 2.x, merchants can now share 150 data points with issuers, helping them to make more informed risk decisions. The key to capitalising on this expanded scope is to leverage the most relevant and up-to-date intelligence, on a global scale, across industries, channels and platforms.

Harnessing a network of global intelligence, updated in near real time

Issuers face the balancing act of maintaining high approval rates while streamlining a customer experience that has previously been criticised for unnecessary friction and an over-reliance on passwords.

Issuers and ACS providers therefore need access to the most comprehensive, relevant intelligence to authenticate a cardholder in near real time, minimising additional stepups and optimising the use of low-friction authentication strategies when required.

LexisNexis® Risk Solutions provides that edge via digital identity intelligence harnessed from thousands of global digital businesses, across over 50 billion global transactions, updated in near real time.

The LexisNexis® Digital Identity Network®

The ability to attach historical context to a cardholder's device, location, email address and online behaviour, even when they are interacting with 3DS 2.x for the first time, is critical for success.

55B
Transactions Processed 2020

2B
Digital Identities

5B
Devices

1B
Email Addresses

Intelligence available from the LexisNexis® Digital Identity Network®

Digital Identity Intelligence:

- Trust, risk, anomalies, linked identities, age of digital identity, email risk assessment, identity data

Device Intelligence:

- 3 different device identifiers, device characteristics such as operating system, model, browser, plugins

Location Intelligence:

- Country, city, connection type, presence of VPNs, TOR and proxies

Threat Intelligence:

- Malware, remote access trojans (RATs), emulators, cloned devices
- Global lists of confirmed fraud, block lists, money mules

Behavioural Intelligence:

- Gestures, behaviour changes, mouse movements, special keys
- Transaction details such as amount, velocity, beneficiary details, times

Integrating LexisNexis® Risk Solutions with ACS providers to make more informed risk decisions

Intelligence from the Digital Identity Network® can provide an enhanced view of trust and risk throughout the card-not-present (CNP) 3DS customer journey. These fraud and authentication capabilities are already being used successfully by a number of issuing banks and financial institutions, in partnership with a range of access control service (ACS) providers.

The three integration options are:

1. LexisNexis® Risk Solutions acting as the primary fraud risk engine for a third-party ACS (via its LexisNexis® ThreatMetrix® product).
2. LexisNexis® Risk Solutions acting as an additional data feed into existing ACS fraud risk engines to augment risk decisioning.
3. LexisNexis® Risk Solutions acting as an authentication layer within the 3DS challenge journey, including a range of Strong Customer Authentication (SCA) based solutions.

1. Acting as the primary fraud risk engine

In the 3DS ecosystem, LexisNexis® ThreatMetrix® can be used as the fraud risk engine for an ACS provider. ThreatMetrix is an identity verification, fraud prevention and authentication solution that operates across the online customer journey. It can verify new account openings and authenticate account lifecycle management transactions, reliably identifying trusted users from potential threats.

BENEFITS

- By choosing to leverage ThreatMetrix technology during the 3DS journey, issuers can benefit from global digital identity intelligence that is updated in near real time.
- As well as having the ability to consume the data sent to the ACS by the merchant (the Areq), ThreatMetrix also harnesses proprietary data from the Digital Identity Network, to augment the decision-making process. As mentioned above, this data includes detailed device, location, behaviour and threat intelligence.
- Using this data, ThreatMetrix creates individual digital identities for every transacting user, intricately understanding how every cardholder typically interacts online.
- Understanding a user's device habits, their location habits, their average payment amounts, their typical shipping address to IP proximity and much more, can enable a holistic and complete fraud risk and trust assessment.
- Additionally, using the ThreatMetrix Decision Management Portal, issuers can build and configure their own strategies to manage 3DS transaction risk. These strategies can comprise a set of rules that look for specific information within a transaction and then apply a risk weighting or take certain actions if quantified conditions are met.

The benefit of having an ACS service and ThreatMetrix working together is compelling. Using additional data generated during the risk assessment empowers a higher fraud capture opportunity, while ensuring legitimate users experience a low friction checkout experience.

2. Acting as an additional data feed into existing ACS fraud risk engines

3DS CNP risk decisions are typically made using the data points that are provided within the Areq, which is data provided by the merchant to the issuing bank. The 3DS 2.x spec also expanded the scope of the Areq to enable a more contextualised data exchange, further improving the issuers opportunity to make a reliable fraud decision.

Beyond this, the 3DS 2.x protocol offers a great opportunity for card issuers to collect custom data via the method URL protocol, which can be used to augment risk assessment decisioning capabilities even further. The method URL enables utilisation of enhanced device recognition, digital identity profiling, location analytics, threat anomaly detection via the browser.

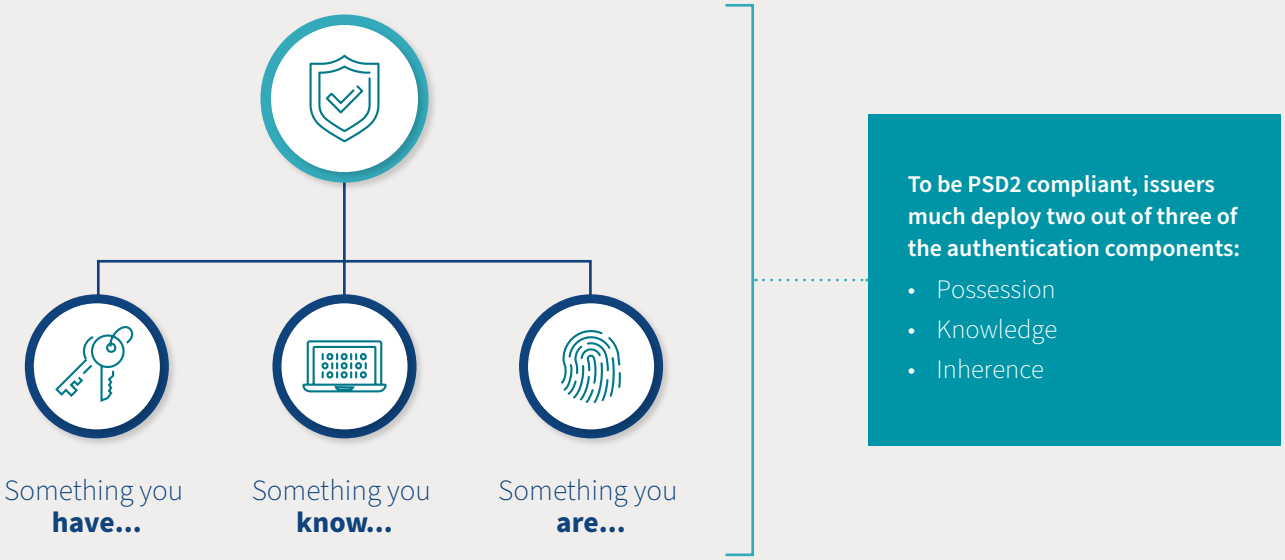
BENEFITS

- By deploying ThreatMetrix capabilities via the method URL, ThreatMetrix can produce hundreds of additional data points (as outlined above) that can be analysed via the ThreatMetrix rules engine.
- This data can be used to augment the overall CNP decision-making capability of the issuers' ACS, empowering increased fraud capture and reduced false positives.
- ThreatMetrix can provide not only raw data, but also optimised, scored risk assessments, into the existing fraud engines of ACS providers.
- Opting to feed ThreatMetrix data into its existing ACS engine would enable an issuer to make a more contextualised risk decision with fewer unnecessary cardholder challenges and increased fraud detection opportunity.

3. An authentication layer within the 3DS challenge journey

The Second Payment Services Directive (PSD2) mandates Strong Customer Authentication (SCA) measures within the CNP challenge journey. LexisNexis® Risk Solutions has developed a range of both inherence and possession factor capabilities to enable issuers to authenticate their users in compliance with regulatory guidance, while maintaining a low friction user experience.

SCA Components



The following authentication solutions can be layered to optimise a PSD2 compliant, low friction authentication journey, reserving more expensive step-ups for high-risk transactions.

Device Binding: ThreatMetrix Strong ID creates a cryptographic bid between an end user's web / mobile browser / app and ThreatMetrix for persistent and secure device recognition. This is currently being used by several organisations as part of a SCA workflow.

- **Silent and low friction following the first bind**
- **Very cost effective for high volume transaction**

SMS OTP: An out-of-band authentication method delivering a time sensitive, unique random passcode via SMS, email or phone call. This is assured by SIM swap / redirect and porting data.

- **Secure**
- **Can be used for customers who don't have a mobile app registered**
- **Ability to include dynamic linking**

Push Notification: Utilises an end user's mobile device, specifically the mobile app, as a form of out of-band authentication during browser based transactions. It uses the standard iOS or android secure push notification services.

- **Low friction for customers who have a mobile app registered**
- **Ability to include dynamic linking**

Knowledge Based Authentication: Built with intelligent algorithms and accessing billions of consumer records, KBA dynamically develops personal questions and multiple answers to authenticate a user's identity.

- **Something you know without having to recall a password**

LexisNexis® TrueID®: The user's identity documents are scanned, the identity is then validated, and enrolled into the TrueID database.

- **Reliable authentication of physical entities**

Behavioural Biometrics: Using the behavioural biometrics data collected upon input of the SMS OTP to provide a second factor of cardholder authentication in a 3DS 2.x workflow.

- **Silent and low friction approach to layer with another compliant authentication strategy**
- **Very cost effective for high volume transactions**

Example: Layering the OTP response (possession) with behavioural biometrics (inherence) for a SCA compliant 3DS workflow

Behavioural Biometrics is the term used to describe the way an online user interacts with a desktop, mobile or laptop device via their keyboard, mouse and/or touchscreen.

LexisNexis® Risk Solutions developed its behavioural biometrics capability to add an additional layer of intelligence to distinguish high-risk from trusted behaviour. This has been extended to authenticating returning users as part of the 3DS 2.x challenge flow.

Behavioural biometrics data is collected while the cardholder is entering their SMS one-time passcode (OTP) on the issuer's challenge page. An API call can then be made by the issuer to retrieve a near real-time authentication decision.

In conjunction with the SMS OTP response, the behavioural biometrics authentication decision creates the second factor of authentication required to satisfy the SCA protocol.

Despite the fact the data collection opportunity on the SMS OTP journey can be perceived as minimal, initial results have demonstrated data collected can reliably compare the current transaction to the cardholder's existing behavioural profile.

BENEFITS

- A low-friction approach to meeting the SCA regulatory requirements
- Removes the requirement for cardholders to remember passwords, which are associated with higher volumes of cart abandonment
- Continuous enrichment of cardholders' behavioural profiles
- Transparent machine learning model output
- Customisable requirements to baseline user behaviours and overall authentication confidence

Conclusion

Partnering with LexisNexis® Risk Solutions can enhance the data available to ACS providers when making fraud decisions. The ThreatMetrix product can also become the primary transaction risk assessment engine if required. As a solution already deployed at many financial services organisations globally to protect online banking sessions, embedding ThreatMetrix within the ACS flow can enable closer shared intelligence across all digital banking channels, and provide a single customer view across the bank.

LexisNexis® RISK SOLUTIONS

To find out how we can help you and your business,
call 029 2067 8555 or email uk-irl-enquiry@lexisnexisrisk.com

risk.lexisnexis.co.uk/fraud-and-identity-management