EMERGING PAYMENTS ASSOCIATION

“Issuer Declines”: The impact of SCA on payments users

A White Paper on the impact of Strong Customer Authentication strategies on the experience of payments users and what this means for the industry.

Sponsored by

CHARGEBACKS911
CHALLENGE THE STATUS QUO

With a 14th September compliance deadline looming, UK issuers have embarked on implementing Strong Customer Authentication (SCA) measures, a requirement of the European Union PSD2 directive that is meant to boost payments security...

58% of the 13 UK issuers surveyed for this study think that too much friction is being imposed on the payments experience by the new regulations. Especially since the SCA requirements are expected to affect the speed of consumer transactions and the number of steps to be completed when paying.

Should merchants be planning for the introduction of SCA? Issuers definitely think so as the new regulations will have a significant impact on the user experience (UX), particularly for eCommerce transactions.

Consequently, once implemented, issuers predict that in the short term the number of transactions declined will increase from today's 3% to between 20-30%. While the number of step-up authorisation requests is expected to range between a third and half of all online transactions.

The top 3 authentication approaches being explored by issuers include; One Time Passwords (OTP) with delivery via SMS to a mobile phone, Authentication within a mobile banking app, and the use of 3DS technology. However OTP and 3DS authentication is expected to have a negative impact on the UX.

Biometrics are expected to have a lower impact on the UX but these will not initially be supported by many issuers.

The study also found that there is limited support of 3DS v2.1 today. Despite this, 66% of surveyed issuers expect to be ready by the end of 2019. 3DS v2.1 has an advantage over 3DS v1 because it has a surety of satisfying SCA legal requirements.

Issuers face a myriad of challenges including the need to juggle SCA demands with other business priorities and regulations, as well as complying within the stipulated timeline.

All this is exacerbated by delayed feedback when seeking clarifications on issues, such as whether Merchant Initiated Transactions were to be deemed out of scope for SCA (where feedback took 8 months).

The study also highlights merchant challenges including a lack of awareness of the need for SCA compliance, especially for small and medium-sized enterprises who form the majority of merchants.

In tackling chargebacks, the Visa Claims Resolution programme showed positive results, reducing dispute resolution time by 15%. Furthermore, a majority of issuers reported that the number of chargeback disputes has stayed at the same level as one year ago. The main reasons given for declining transactions include insufficient funds and invalid card details/ expired card; soon to be added to this list will be lack of customer authentication. The key to SCA is to ensure a smooth transition for businesses to take their consumers on the right journey. It's vital that payment providers, such as Judopay, are included in SCA implementation and communication programmes.

Siobhan McGinley

Siobhan McGinley
Project Lead for Transaction Insights
Head of Marketing
Judopay

About Payments Consultancy Ltd

Payments Consultancy, the commissioned researcher and author of this white paper, is an award winning independent payments consultancy that advises retailers, hospitality providers, banks, acquirers, issuers, payment providers, and investors.

Payments Consultancy provides specialist advisory services related to:

- Strategy development
- Regulatory advice
- Market assessments
- Competitive analysis
- Supplier selection
- Commercial due diligence services

Payments Consultancy's primary consultant is Mark McMurtrie who has over 25 years payments experience including in mobile, face-to face, ecommerce, Omni-channel and instant bank payments. Mark is an ambassador for the Emerging Payments Association, industry commentator, conference chairman, popular speaker and awards judge.

www.payments-consultancy.com

About the EPA

The Emerging Payments Association (EPA), established in 2008, connects the payments ecosystem, encourages innovation and drives profitable business growth for payment companies. Its goals are to strengthen and expand the payments industry to benefit all stakeholders.

It achieves this by delivering a comprehensive programme of activities for members with help from an independent Advisory Board, which addresses key issues impacting the industry.

These activities include:

- A programme of 70 events annually
- Annual Black-Tie award ceremony
- Leading industry change projects
- Lobbying activities
- Training and development
- Research, reports and white papers

The EPA has over 150 members and is growing at 30% annually. Its members come from across the payments value chain; including payment schemes, banks and issuers, merchant acquirers, PSPs, merchants and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.

www.emergingpayments.org

Table of Contents

To find out more information on this SCA research or Project Transaction Insights, please contact info@emergingpayments.org.

1. Executive Summary

Merchants are directly impacted by issuer authentication and authorisation strategies but often have little understanding of what these are. These strategies can have a significant impact on the customer user experience and result in lost revenue. We have asked UK issuers about their plans and in this white paper are pleased to share these details with you.

The key findings are as follows:

- ECommerce card payment fraud costs the UK £310 million annually.
- Regulators have determined that enhanced security needs to be implemented including the adoption of Strong Customer Authentication to tackle this growing problem.
- These changes are in many aspects as significant as the introduction of Chip and PIN.
- The planned additional friction may well lead to higher basket abandonment rates and lost customers and in the short term a worse user payments experience.
- Unless a managed roadmap is agreed SCA is expected to see step-up authentication requests increase from 2% to 30-50% and transaction declines rise from 3% to 25-30%
- The key approaches issuers will use are 3DS v2 technology, One Time Passwords delivered by SMS, in-app authentication and biometrics.
- Merchants should implement 3DS v2.1 as soon as possible despite any poor experience of 3DS v1 and move to 3DS v2.2 without delay.
- Without FCA agreement to a managed roadmap issuers will be forced to decline transaction without an authentication or exemption. Therefore make sure transactions have the right flags and indicators.
- The entire payments ecosystem is not ready and needs more time before active enforcement starts. An 18-month roadmap has been proposed, but this has not yet been agreed.
- Customer and merchant awareness levels need to be significantly higher. SMEs are currently largely unaware of the upcoming changes.
- The long term SCA strategic solution calls for biometrics and 3DS v2.2+
- All payment industry stakeholders are calling for consistency across Europe and decisions from national CAs are awaited.
- Merchant Category Codes will have growing importance and so check the right one is being applied.
- Merchants generally receive a high quality electronic authorisation service with over 75% of issuers delivering >99.99% availability.
- New authorisation services, like realtime notifications and temporary card freeze, are being introduced to allow improved self-management of accounts and to reduce fraud.
- Effective chargeback management tools are required. ■

> “We will be forced to decline any transactions that has not been authenticated or allowed an exemption.”
>
> - Large card issuer

2. Introduction

The customer payments experience is significantly impacted by the authentication and authorisation strategies determined by a card issuer. In order to tackle escalating levels of payment card fraud, which totalled £566 million last year, regulators have demanded compliance with new stricter strong customer authentication (SCA) requirements as part of the European PSD2 regulations. Issuers are at the same time adopting enhanced authorisation strategies and both of these will impact all merchant categories but particularly those selling online.

> “ACTION HAS TO BE TAKEN TO TACKLE ESCALATING FRAUD LEVELS”
>
> - ISSUER

SCA requires multi factor authentication in order to ensure the payer is genuine and not a fraudster. These must come from two of the following three categories, Possession (something you have), Knowledge (something you know) and Inherence (something you are). Plus the authentication must be dynamically linked to a particular transaction. Issuers and Acquirers are obliged by UK law to comply with these European requirements set by the European Banking Authority (EBA) and compliance will be monitored by the Financial Conduct Authority (FCA) who are the UK's competent national authority (CA)

> “THE MILLION DOLLAR QUESTION IS HOW WILL ISSUERS ENFORCE SCA IN SEPTEMBER. WILL ALL TRANSACTIONS BE DECLINED?”
>
> – MERCHANT ACQUIRER

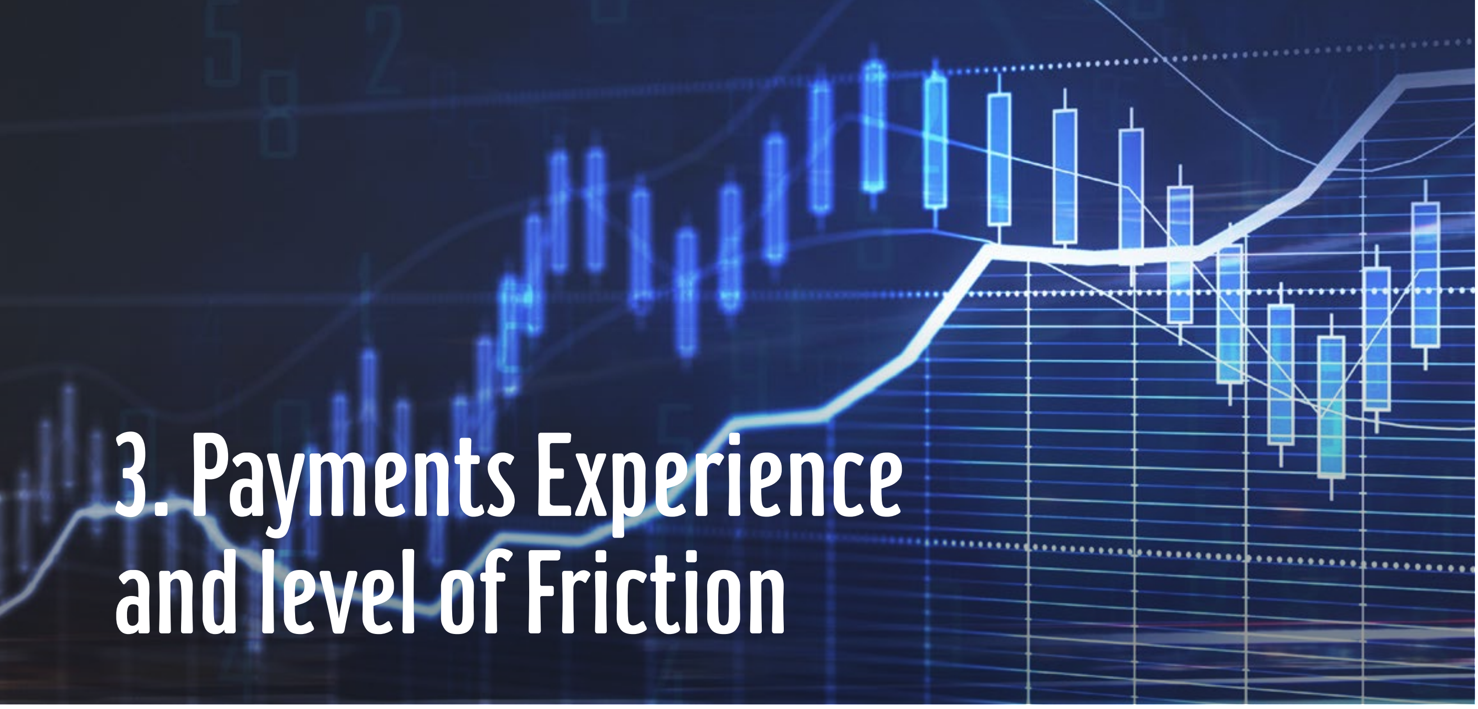
Merchant awareness levels are extremely low, technical requirements have been late to be agreed, and solution availability is limited. The entire payments value chain from the merchant, through the gateway, acquirers, payment networks, right up to the issuer must be ready for these changes. The PSD2 Regulatory Technical Standards (RTS), which specify these SCA requirements, require strong customer authentication to be completed or else the issuer must decline the payment transaction.

Acquirers may be allowed to claim an exception to this standard, providing their chargeback and fraud statistics remain below the minimum threshold (set by the EBA). Merchants must oblige with their acquirer's requirements, which will translate to added friction and invariably higher cart abandonment.

This first of its kind research finds out how UK card issuers intend to implement SCA, learns which methods they will be using, hears about their state of readiness and assesses the likely impact on both merchants and cardholders.

During the months of April, May and June we spoke to 13 UK issuers, including 3 of the 4 largest, with credit, debit and prepaid card portfolios. Collectively these organisations issue over 107 million cards with a 61% market share and therefore the results are representative of the overall market position.

This research has found a distinct lack of market readiness amongst all key stakeholders. ■



3. Payments Experience and level of Friction

The consumer payments experience is influenced by many factors including the choice of payment options, the speed of processing and the number of steps that have to be completed. Amazon has calculated that each additional click increases basket abandonment rates by 15%. The market requires a highly intuitive user experience and for payment processing to be integrated seamlessly with other business applications.

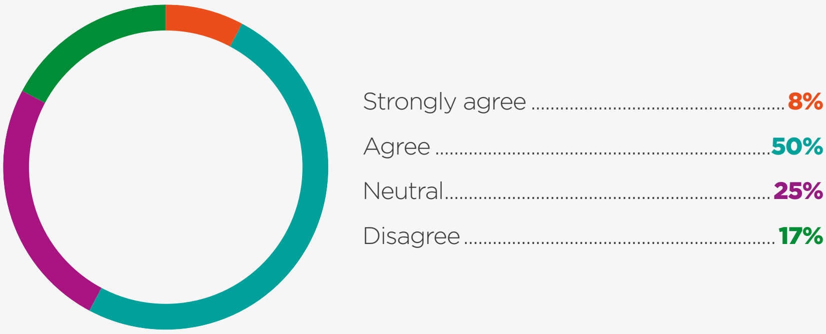
> "EACH ADDITIONAL CLICK INCREASES BASKET ABANDONMENT RATES BY 15%"
>
> – AMAZON

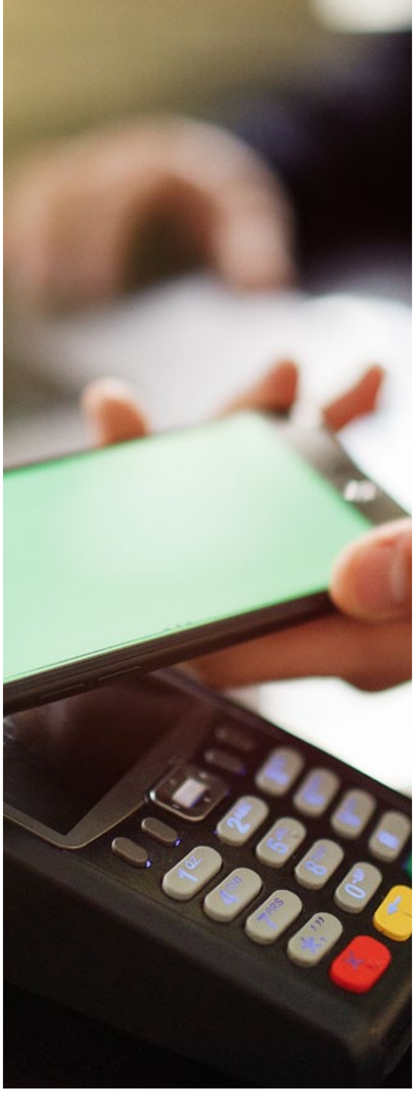
Over recent years great efforts have been put into improving the payments experience and removing friction without compromising security. The increasing adoption of contactless, NFC mobile payments, and one-click checkout experience is all proof to this point. Merchants have mixed views on 3DS due to poor experiences with early v1 implementations which resulted in 10%/12% basket abandonment rates across Europe. However there have been significant improvements to the payments experience with 3DS v2 including the use of One Time Passwords (OTP) and biometrics instead of static passwords, support for smaller device screens not just desktop browsers, supporting in-app and non payment authentication, avoiding slow URL page redirection, maintaining merchant branding and avoiding auto enrolment during a purchase.

Users are demanding a great payments experience and not tolerating extra hurdles or delays being placed in their path. Merchants know that additional friction, unless implemented extremely well, will result in abandoned sales both online and in-store. In today's highly competitive retail environment no business can face loss of revenues from disgruntled customers who

> "WE ARE NOT IN THE BUSINESS OF DECLINING TRANSACTIONS, BUT WILL BE FORCED TO DO SO IN ORDER TO SATISFY REGULATORY REQUIREMENTS"
>
> – DEBIT CARD ISSUER

Is too much friction being introduced?





> “MERCHANTS SHOULD NOT BE PUT OFF BY ANY BAD EXPERIENCE OF 3DS v1”
>
> – INTERNATIONAL PAYMENT NETWORK

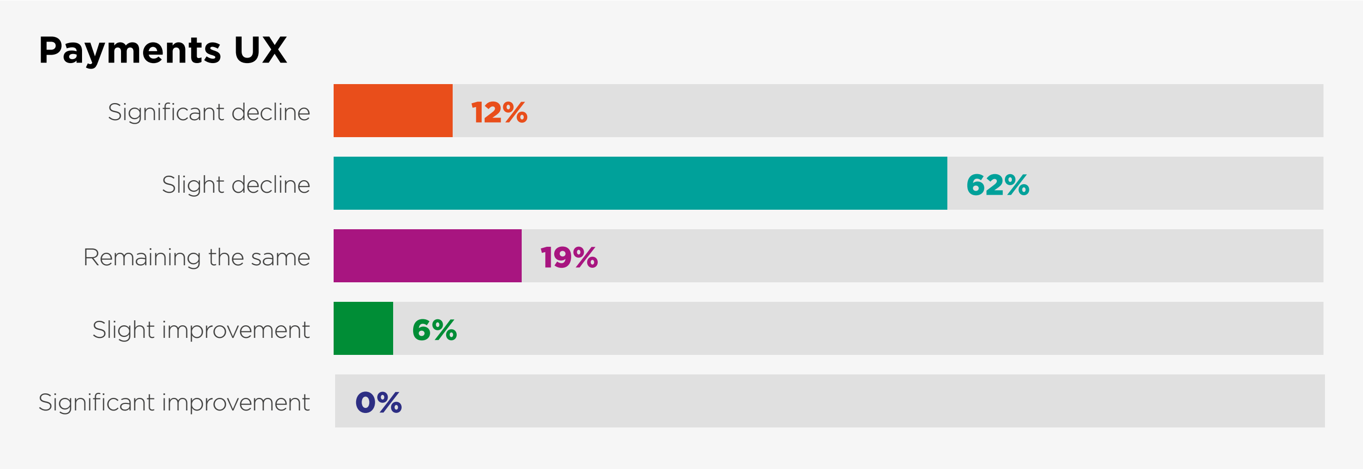
express their annoyance through basket abandonment or walking out of stores. Merchant acquirers are sympathetic to the impact on merchants and will help allow the maximum and smart use of SCA exemptions.

Our research found that 58% of issuers agreed or strongly agreed that too much friction is being imposed on the payments experience with new regulations such as SCA. 25% held a neutral opinion with only 17% disagreeing.

Stakeholders need to work together to ensure an optimal balance is established between controlling fraud without ruining the payments experience. Issuers told us that the additional friction being introduced into the payments experience is necessary in order to control the escalating customer not present fraud losses, which currently total £310 million.

As regulated entities issuers have decided that they must accept the short-term pain of annoying customers, in order to comply with the law, reduce fraud losses, maintain consumer confidence and ensure long-term survival of the card payments business model. We asked about the likely impact of strong customer authentication and heard that 74% of issuers expect SCA to contribute a negative impact in User Experience (UX). ■

> **“We have worked hard to improve the user experience and reduce friction but now fear a significant decline”**
>
> **- International retailer**



4. Strong Customer Authentication

All issuers are busy preparing for the introduction of SCA. They can make their own choice on which authentication methods they decide to support and therefore the UX will not be consistent and it will take longer for customers to become familiar with the new payment steps. SCA applies to all sales channels but will have most impact on ECommerce transactions. Chip & PIN technology largely delivers SCA for face-to-face transactions although there are some changes required to authorisation message fields and the handling of contactless transactions as counts and limits have been imposed.

Impact

Our research shows that SCA is going to have a very significant impact on eCommerce transactions. These will see a substantial increase in the numbers of step-up authentication requests.

Currently issuers request this for only 2% to 4% of their eComm transactions, normally as a cardholder you just see the pop-up box appear, watch the engine whirl around, but you are not required to take any action. However; once SCA compliance is required, issuers expect between 30-50% of online transactions to face a step-up authentication request. It is also predicted is that the number of transactions being declined will increase in the short term from today's 3% to between 25-30%, a significant cause for concern, especially for merchants. If more time is available before active enforcement then these decline rates will be lower. These dramatic increases in step-up requests and declines will come as a big surprise to consumers and have a significant negative impact on the payments experience. It will also cause big issues for merchants with higher abandonment rates and loss of revenue anticipated.

> “WE EXPECT 30-50% OF ECOMMERCE TRANSACTIONS TO REQUIRE STEP UP AUTHENTICATION AND 25-30% TO BE DECLINED”
>
> – TRADE ASSOCIATION

> “SCA WILL HAVE A MAJOR NEGATIVE IMPACT ON OUR REVENUES AND CUSTOMERS. IMPLEMENTATION TIMESCALES HAVE BEEN TOO SHORT AND MANY QUESTIONS REMAIN OUTSTANDING”
>
> – INTERNATIONAL HOTELIER

One year after the September 19 compliance deadline issuers expect the number of step-up authentication rates to continue to be in the 30-50% range but the proportion of transactions being declined to reduce to 10% as the ecosystem completes readiness status and consumers become more familiar with the new requirements. This predicted reduction in declines is to be welcomed however merchants should note that this would still be at 3 times today's level.

Without a roadmap

eComm Txns	June 19	Sept 19	Sep 20
Step-Up requests	2%	30-50%	30-50%
Declines	3%	25-30%	10%

Authentication approaches

We found that the top approaches initially being adopted for SCA compliance are One Time Passwords (OTP) with delivery via SMS to a mobile phone as a knowledge element, Authentication within a mobile banking app, card data as a possession element and use of 3DS technology. Issuers said that they expected OTP and 3DS to have a major negative impact on the UX, with biometrics being seen to have a lower, minor, impact. Most issuers are planning to make greater use of Artificial Intelligence (AI) and as this technology matures a greater positive impact on the payments experience can be expected.

Currently 48% of bank customers use mobile banking services and 16% are registered with Apple Pay, Google Pay or a similar service. This means that issuers need strategies for both digital ready customer groups and those who have not yet made this transition. Our interviews highlighted a common issue for legacy credit and debit card issuers

“OTP BY SMS IS A KEY PART OF OUR SCA IMPLEMENTATION PLANS. IT WILL TAKE TIME FOR OUR CUSTOMERS TO ADOPT BIOMETRIC AUTHENTICATION OPTIONS”

– CREDIT CARD ISSUER

that of poor quality customer mobile phone and email address data records. They are actively seeking to ensure they have up to date and accurate customer contact details, but are finding low levels of customer engagement and some resistance to providing these through fear of receiving unwanted marketing approaches.

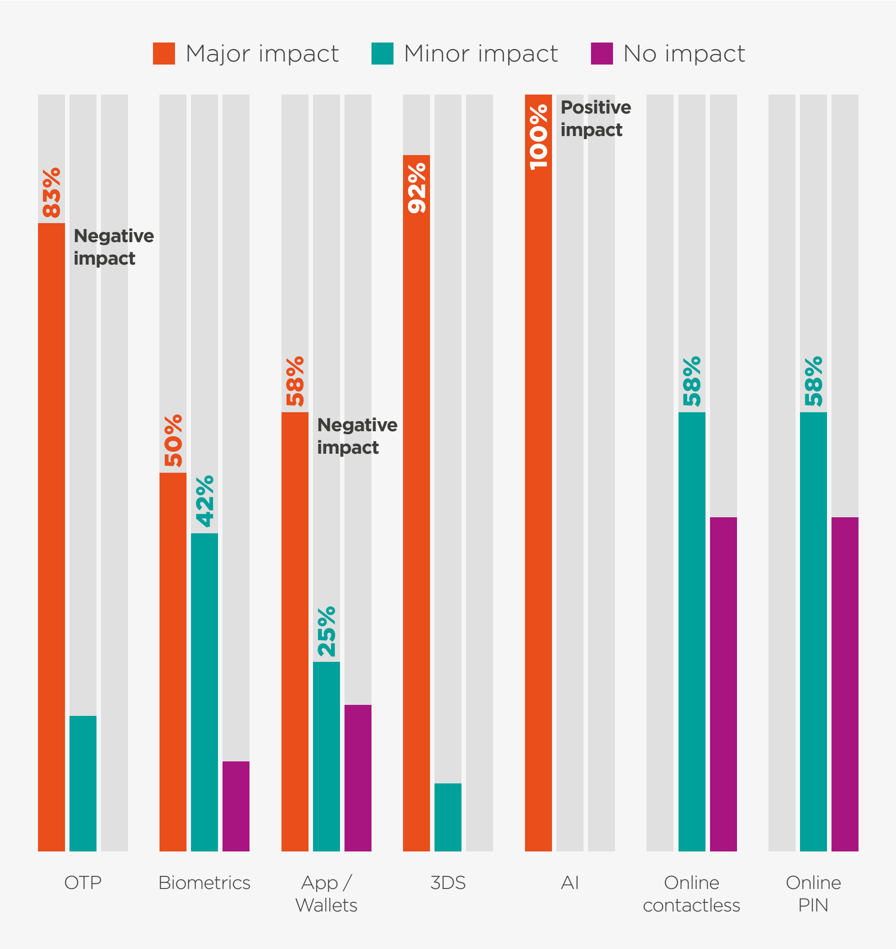
The FCA has warned issuers that they must not overly rely on a single authentication method and must not exclude customer segments who may not have mobile phones or network coverage. This may stimulate the use of a broader range of methods and allow customers to advise their authentication preferences.

In late June, as we finalised our research, the EBA advised, and the FCA subsequently ratified, that card details could not be considered as either a possession or knowledge factor, that OTP was restricted to proving possession and that data points provided through 3DS v2 protocols cannot be considered as inherence elements. Previously the RTS had taken a technology neutral approach.

With less than three months before the September compliance date the industry is now reassessing its plans as a matter of urgency and will need to accelerate plans to support biometric options. The net result of this EBA ruling on acceptable authentication

“AWARENESS LEVELS ARE UNACCEPTABLY LOW AMONGST CONSUMERS AND SMEs. COMMUNICATION PROGRAMMES NEED TO BE RAMPED UP AND CO-ORDINATED”

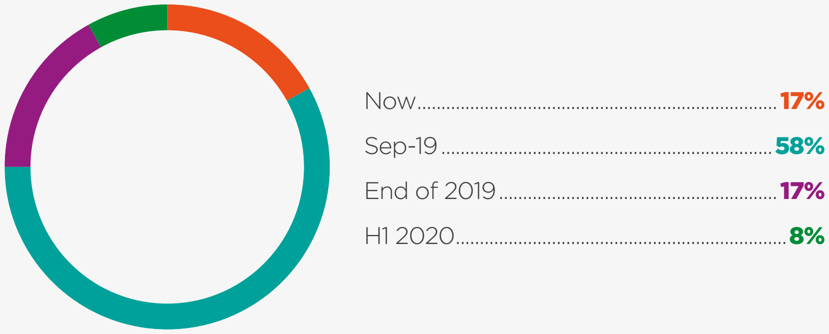
– TRADE ASSOCIATION



methods will be accelerated support of biometrics, which was previously not going to be used until later phases.

It is now unclear which authentications methods issuers will elect to use for those customer segments who are not mobile banking app users or owners of a smartphone. They appear to favour to continue with existing plans for use of SMS OTP and see this as their preferred accessible solution. Hardware based card authenticator devices could be the answer but this is seen by many to be a backward step and unattractive option. As each issuer will make their own selection we can expect a lack of consistency and differing payment experiences.

Compliance readiness status



Readiness status

We asked issuers to report on their state of SCA readiness. 17% said they are ready today out of a total of 75% who expect to be so by the 14th September 2019, with a further 17% by the end of 2019. The percentage of issuers who are ready now is higher than 17% as progress has been made since the research was conducted. The small remainder plan to be compliant during the first half of 2020. But 50% told us that they wont be able to support all SCA exemptions in 2019. This highlights the difference between minimal (legal) compliance status and optimal compliance, which is shown by operational readiness. For merchants it is worth highlighting that an issuer's enforcement approach is far more significant than actual compliance readiness. A major concern of issuers is predicting the resource levels that will be required at contact centers to handle customer calls following the anticipated increase in transaction declines and confusion from step-up authentication requests. Retailers propose that issuers should not be declining transactions until they have up to date contact numbers for all customers, otherwise they feel their efforts to deliver compliance will be ignored.

> "CUSTOMER ARE PROVING RELUCTANT TO SUPPLY UPDATED CONTACT DETAILS"
>
> - LARGE CARD ISSUER

> "OPERATIONAL READINESS WILL NOT BE IN PLACE FOR SEPTEMBER. ALL STAKEHOLDERS NEED MORE TIME BEFORE ACTIVE ENFORCEMENT"
>
> - PAYMENTS CONSULTANT

3DS technology

50% of UK eCommerce merchants have adopted 3DS v1 and this version is believed by many to meet minimal SCA compliance as it supports two-factor authentication and dynamic linking. On average v1.0 has a 10-12% transaction abandonment rate, which is one the many reasons retailers do not love it. Of significance is that 30% of issuers' say they are currently planning to decline all v1.0 transactions for fear that the regulator may deem these to be non compliant.

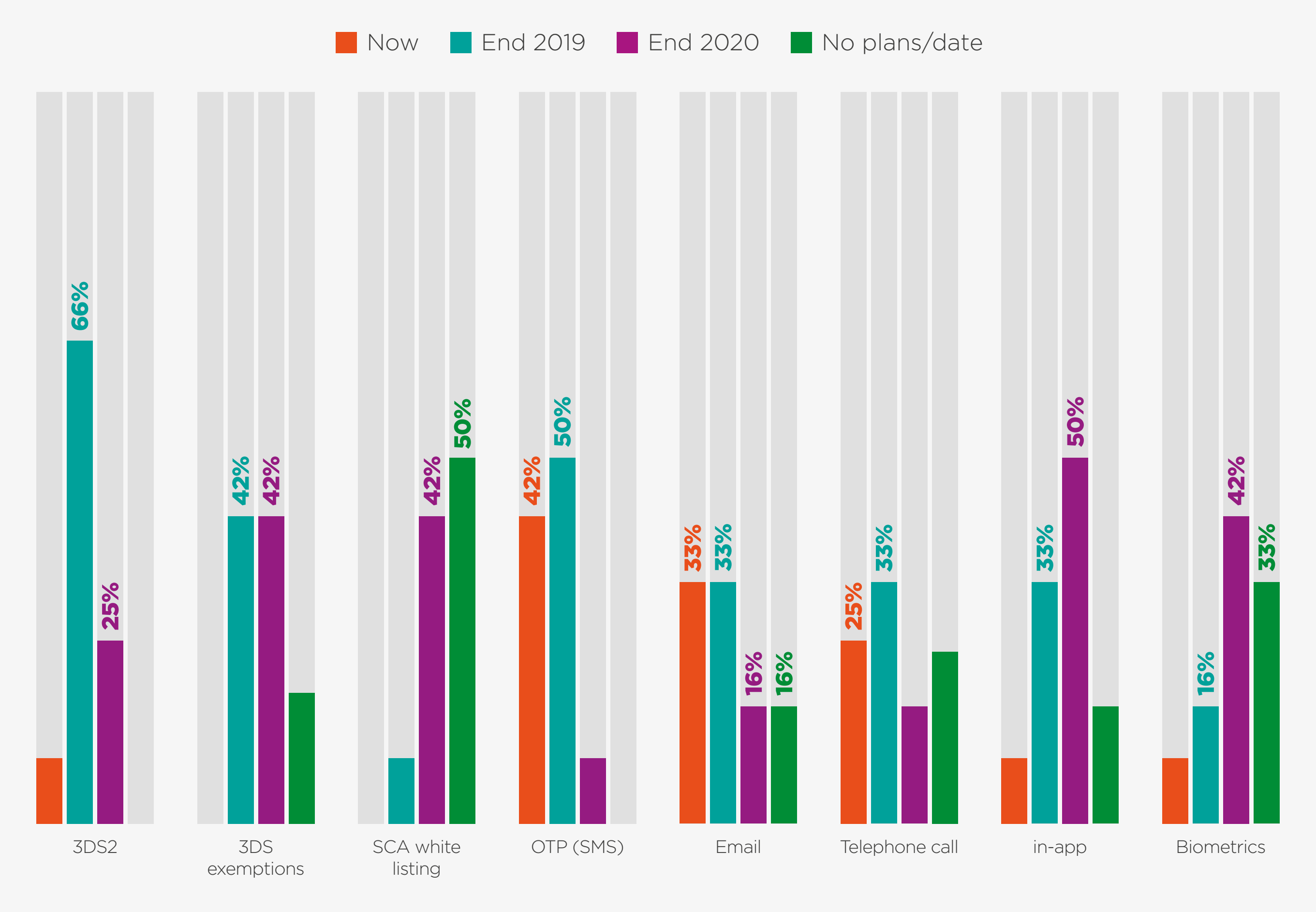
They require regulatory certainty in order to stop unnecessarily declining transactions. Mastercard advocate that merchants should be implementing v2.1 now, with support for their defined additional fields, because this version definitely satisfies SCA legal requirements, as it additionally delivers mobile device compatibility, non payment authentication, enhanced data sharing, biometric authentication capacity and partial support for merchant initiated transactions (MIT).

Many organisations will not be operationally ready for 3DS v2.2 until 2020. Representing the merchant viewpoint the BRC promotes delayed enforcement until v2.2 can be implemented as only this version includes full support for MIT, trusted beneficiaries, additional device compatibility and 3RI cryptograms that are required for efficient authentication within mobile banking apps. 3DS v2.2 therefore delivers optimal SCA compliance.

Retailers want to avoid the additional costs and disruption of having to implement multiple versions. Issuer support for 3DS v2.1 has been delayed by late product delivery giving little time for merchants and gateways to complete testing. However 66% expect to be ready by the end of 2019, despite only 42% expected to be able to accept SCA exemptions this year. Support for white listing of trusted beneficiaries will not be generally available from most issuers until 2020 at the earliest.

Biometrics

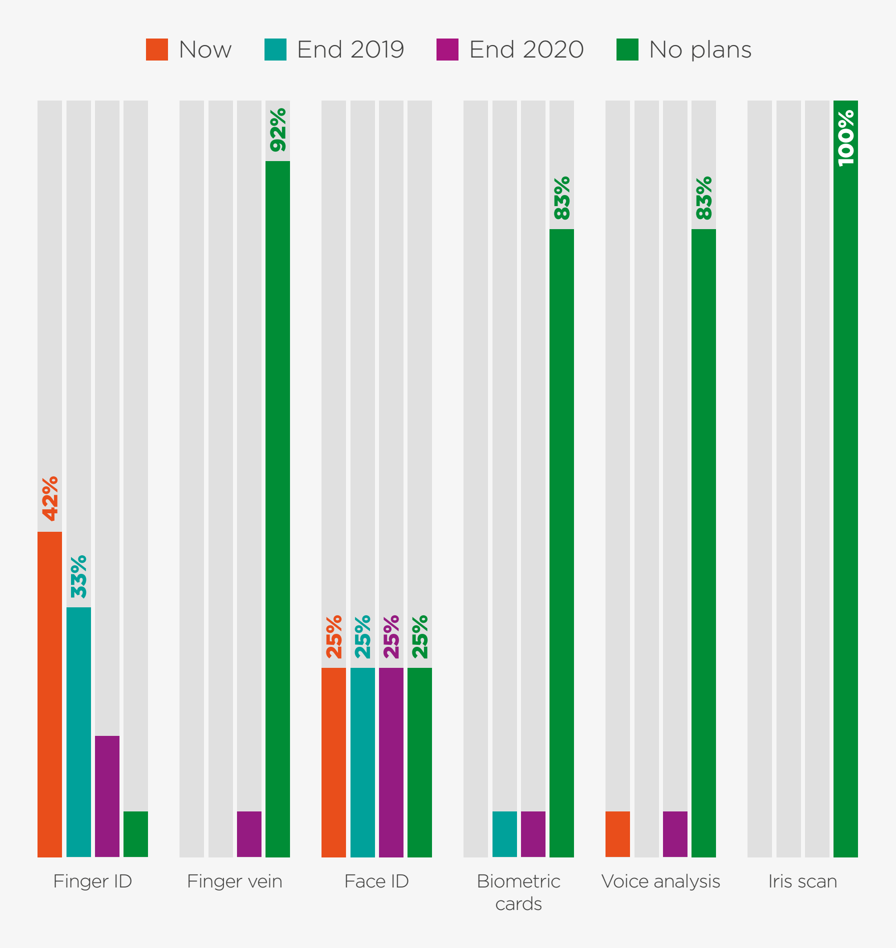
> "ONE OF THE FEW CERTAINTIES IS THAT 3DS v2 NEEDS TO BE ADOPTED AS FAST AS POSSIBLE"
>
> - CREDIT CARD ISSUER



Future biometrics is seen to be key to delivering a great SCA compliant UX by the majority of issuers. Fingerprint scanning and Face geometry appear to be the most promising initial methods partly due to the support of these technologies by the big technology providers Apple, Google and Samsung.

We asked about the potential issuance of biometric cards, but most issuers told us that due to the higher costs, immaturity of the technology and current supply chain capacity, that significant rollouts are unlikely to be seen before 2021. Small pilot programmes targeting niche portfolio segments will start appearing in 2020. Some large issuers told us that they see little potential for biometric cards as card fraud levels in a face to face environment are low and under control.

In light of the recent EBA ruling on compliant SCA elements issuers are required to accelerate their support for biometrics Merchants are advised to implement 3DS v2.1 now and then migrate to v2.2 once solutions are fully tested and available.



Knowledge elements	Possession elements	Inherence elements
Password	Device evidenced by OTP	Fingerprint scanning
PIN	Device evidenced by Token	Voice recognition
Challenge questions	Card/Device evidenced by QR	Vein recognition
Passphrase	Card evidenced by reader	Hand/Face geometry
Swiping path	Card evidenced by dynamic Card Security Code	Retina/Iris scanning
	App/Browser evidenced by device binding	Keystroke dynamics
		Heart rate/Body movements
		Angle device held

EBA compliant authentication elements

The table above confirms the current EBA viewpoint on each of the acceptable authentication methods within each of the three categories. They have clarified that the following cannot be used as knowledge elements: email address, user name, card details (printed on card) and an OTP generated by, or received on, a device. For possession elements: an app installed on the device, card details printed on the card and card evidenced by a printed OTP list are not acceptable. In the Inherence element list: a memorised swiping path and information transmitted using a communication protocol such as EMV 3DSecure are also deemed to be non compliant. Questions have been raised why static passwords, which are inherently poor from a security and UX perspective, are acceptable, whilst static card details are not.

Exemptions

Issuers and acquirers may dramatically improve their ability to manage SCA requirements, by maintaining an exemption status. All of those surveyed intend to allow maximum use of SCA exemptions in order to reduce the negative impact on merchants and customers. Exemptions include: Transaction Risk Analysis (TRA), low value remote transaction, contactless, trusted beneficiaries, unattended transit and parking environments, commercial cards and recurring transactions.

The EBA recommends that a smart approach is taken to requesting exemptions and has provided TRA exemptions for both the acquirer and issuer.

Acquirers have placed concerted effort to reduce fraud rates. The top three initiatives for reduction efforts for UK Acquirers is:

- Enhanced risk management and fraud detection software,
- Integrating with Visa's Merchant Purchase Inquiry (VMPI); a real-time chargeback prevention tool that resolves cardholder complaints to prevent fraud disputes, and
- Enhanced merchant fraud and chargeback reporting tools (e.g. web portals that provide fraud feedback and interaction capabilities).

According to the EBA, fraud reduction may also be achieved through evidence of Friendly Fraud. Friendly Fraud is a type of fraud commonly committed by the cardholder (either unknowingly or intentional), which results in an undeserved refund through the issuance of a chargeback. In the event that an acquirer can prove the occurrence of friendly fraud, their fraud rates will be proportionately reduced; effectuating a greater propensity to achieve exemption status.

Chargebacks911, the first remediation company to enter Europe and leading thought leader on this subject, cautions acquirers to invest in their chargeback management process.

A common challenge among acquirers is the ability to identify Friendly Fraud. Due to its nature being divulged through a tedious and often manual re-presentment process (the process by which a merchant disputes a chargeback by submitting their documentation for review), acquirers are confronted with scaling challenges and often lack the digital competency to reap potential SCA exemption benefits.

Providing a more intuitive and automated merchant web portal, for the submission of merchant-initiated, disputed chargebacks; is paving a way forward in streamlining an otherwise unsustainable workflow. Acquirers that invest in better chargeback management tools for their merchants will glean the advantage of reduced fraud and exposed friendly fraud (i.e., attain and maintain SCA Exemption status).

Our research found that issuers do not expect to be able to support white listing requests of trusted beneficiaries in the short or medium term.

Some issuers raised concerns that white listing will discriminate against SMEs and increase the dominance of large eCommerce merchants. It is worth noting that merchants are not able to request white listing on behalf of their customers. Delegation of SCA requirements from the issuer to the merchant through a contractual framework will be attractive to large and sophisticated merchants.

Reference Fraud rate	Exemption Transaction Value
0.13%	€100 / £90
0.06%	€250 / £220
0.01%	€500 / £430

5. Key Challenges

5.1 Issuer key challenges

All stakeholders in the payments ecosystem have faced multiple challenges in ensuring compliance with the PSD2 SCA regulations. This has largely been through a confusion on exactly what changes need to be made as the RTS is clear at a high level but often lacks sufficient detail for implementation purposes.

> “THE NUANCES OF THE REGULATIONS ARE NOT OBVIOUS. DETAILED ANALYSIS AND DISCUSSION IS NECESSARY”
>
> – CREDIT CARD ISSUER

The time line for compliance has also been a major headache for issuers as the RTS was not published until March 2018, whilst PSD2 came into legal force in January 18, and critical clarifications were not released until Autumn 2018 and the most recent guidance on compliant authentication methods came in June 2019. There remain points of substance to be clarified by the EBA and answers to questions submitted many months previously. Perhaps these delays were partly because the regulators have less understanding of the intricacies of how card payments work in practice today as specifications have previously been developed by the international payment brands working either individually or collectively.

> “WITH LESS THAN 3 MONTHS TO DEADLINE WE CANT CHANGE THE AUTHENTICATION METHODS PLANNED”
>
> – MAJOR CARD ISSUER

Issuers have needed to juggle SCA demands with many other business priorities, and regulations requiring compliance. These include PSD2, IFR, Open Banking and Brexit. Achieving compliance has not been helped by the EBA being slow to respond to questions raised. There was an 8-month wait to hear if Merchant Initiated Transactions were to be deemed out of scope. The EBA was advised of the UK plans for authentication methods in December 2018 and this spelt out the intention to use card credentials as an SCA element.

Old legacy systems hamper many of the UK credit and debit card issuers as they lack the flexibility to make changes. No major new issuing functionality has been added since the launch of Chip & PIN in 2006 and subsequently contactless.

“Issuer readiness has been delayed by late ACS solution availability”

- Trade association

Several issuers are also reliant on third party processors, which has reduced their responsiveness and resulted in delays. We heard that at least one year is required by a large issuer to support new authentication and authorisation functionality. Challenger banks and prepaid card issuers have benefitted from not facing these legacy system challenges and so have an easier route to SCA compliance.

We learnt that the primary approach being taken by issuers for eCommerce SCA compliance is the use of 3DS technology. The 3DS v2.1 specifications were released by EMVCo in October 2017, before the RTS SCA had been finalised. EMVCo testing was available from August 2018 allowing integration efforts to commence in November 2018 resulting in the commercial availability of solutions from February 2019.

Issuer readiness has been delayed in the UK by late ACS solution availability. This will not allow much time for testing and appropriate scaling of systems. It is uncertain how many will have live 3DS2 implementations by the 14th September deadline, but most are expected to be compliant before the end of 2019.

The recent ruling by the EBA that data points provided through 3DS2 protocols can not be considered acceptable inherence elements is unwelcome and the latest challenge to be resolved by issuers.

It was quickly recognised by the industry that a 3DS v2.2 specification was needed for optimal SCA compliance in order to cater for additional device compatibility, to support full transaction risk analysis, merchant initiated transactions, trusted beneficiary listings and an enhanced user experience. Mastercard added message extensions to 3DS v2.1 to address many of these aspects. 3DS v2.2 specifications were released in late December 2018. Suppliers have been enhancing products to support these latest specifications and these will then be submitted to EMVCo laboratories for certification followed by integration and PCI compliance. Full commercial solution availability and deployment can be expected in late 2019 and early 2020.

“SOLUTIONS STILL NEED TO BE FOUND TO COMPLEX USE CASES AND THIS REQUIRES GREATER DIALOGUE AND COLLABORATION”

- PAYMENT SCHEME

Most issuers have invested heavily in SCA compliance. However the size of the task has been underestimated by some, resulting in insufficient budget being allocated. In addition to systems changes a major cost item relates to customer education and communication. The larger a card portfolio the higher the bill. Unlike other payment industry initiatives like Chip & PIN, current account switching, or Take 5 to stop fraud, there is currently no centralised managed and funded communications programme for SCA. As we go to press it looks like UK Finance will create a central project team, with staff secondments from banks, in order to deliver SCA.

5.2 Acquirer and Merchant key challenges

Merchants and Acquirers, like issuers, are facing multiple challenges to deliver SCA compliance. The most significant issue is the low levels of awareness amongst the merchant community. One major survey conducted earlier in 2019 by an international payment network reported 75% of European online merchants were unaware of the need for SCA compliance. Another more recent study from the merchant acquirer Stripe found that 60% of European companies with less than 100 employees admitting that they are either unaware of the SCA regulation, unlikely to be compliant before September or unsure of when they will be compliant.

Recent communication efforts from schemes, acquirers, trade associations and solution providers are trying to address this issue and most large merchants are now aware of the need for compliance (the Stripe reports says just 4% of firms with more than 5,000 employees are unaware of SCA), but this understanding remains lacking for the small and medium sized enterprises who make up the largest proportion of merchants.

Both parties consider that they have been given insufficient time to achieve compliance and fear a high risk to revenue from customers abandoning baskets and issuers declining transactions. Retailers have faced confusion at the detailed requirements level. They have become increasingly vocal in stating that 6 months notice, or 3 as it is now, is felt to be far too short an implementation timescale and that a delay to enforcement should be granted.

Many merchants have well established business processes that now require changing in order to meet SCA regulatory demands. These have far-reaching organisational implications and simply can't be changed overnight. Attitude to risk management is one of these areas. A merchant used to be able to decide how much risk they were willing to accept. Now key risk decisions will be taken by issuers irrespective of a merchant's opinion. These issues demonstrate that SCA compliance is far more than just an IT compliance programme. Many questions have been raised about how current use cases and transaction flows may be impacted by SCA and these have taken far too long to be answered. Many remain unanswered and sit on an issues log being managed by UK Finance.

Today many retailers process payments through multiple sales channels and this adds further complexity as SCA compliance is not just an eCommerce issue. Updates are required to authorisation message formats to support SCA fields, exemptions and the optimal handling of contactless exemptions. Acquirers are taxed with the everchanging task of maintaining and updating file formats and message exchanges – where if not done correctly, will lead to increased costs, lost revenues or increased liabilities; or a combination of all three.

Large retailers are often multinational businesses and have been frustrated by differences in approaches and compliance dates found across Europe. As merchants are not FCA regulated entities they do not have to be compliant themselves. However they are now realising how they may be significantly impacted by issuer strategies. The big concern is that issuers will decline all transactions without an authentication. Our research found that this may happen, but is now less likely since the publication of recent FCA guidance. Acquirers and their merchants fear high rates of customers abandoning shopping baskets through forced use of 3DS technology. Reduced transactional conversion equates to lost revenues and ultimately affects both bottom lines. They have long and unhappy memories of the initial 3DS v1 implementations, which today still results in 10%-12% basket abandonment rates. Indeed research shows that 55% of UK merchants have not implemented any version of 3DS. The merchant viewpoint is that they would prefer a 3DS v2.2 implementation as this supports the full range of SCA exemptions and therefore can deliver a good user experience. Less than 5% of UK merchants are on 3DS v2.1 and first commercial availability of 3DS Server v2.2 solutions is not expected until late 2019/early 2020.

Merchants advise that they require at least a 12-month implementation timescale once compliant solutions are available and therefore consider a revised managed roadmap to active enforcement is needed. Preferably this should be consistently applied across all European countries. Otherwise merchants will see different decision making and payments experience dependent on the location of the card issuer, stores and the roadmap they have agreed with their national CA.

Merchants are unhappy that the task of communicating to customers about why new authentication steps are required and more transactions are being declined will largely be left to them to perform. They feel a centrally funded communications programme should be put in place by the financial community (issuers, acquirers and schemes) in order to educate end users. Retailers are particularly keen to minimise inconsistencies in approach between issuers and schemes. ■

6. Roadmap to enforcement

> “We believe more time is needed for the industry to be ready and would prefer a phased implementation”
>
> - Credit and Debit card issuer

Our research found that all parties within the payments ecosystem require additional time in order to effectively implement SCA and be operationally ready with solutions that deliver a good user experience. These findings are in line with other industry forecasts and warnings. In late June 2019 the EBA agreed that national competent authorities (CA) can provide limited additional time and supervisory flexibility for card payments on an exceptional basis to avoid unintended negative consequences. This requires the preparation of a national SCA migration plan, that this plan has been agreed with the CA and that PSPs are executing the migration plan in an expedited manner. The FCA has confirmed that it is working with the industry through UK Finance to establish an acceptable roadmap. There is no change to the 14th September 2019 deadline but these announcements provide issuers with more time before they are forced to decline transactions without a SCA.

This additional time will allow improved merchant and consumer awareness, greater solution availability, ensure compliant authentication elements are used, allow resolution of identified issues, completion of systems integration and changes to business practices. The FCA has advised that it will not take enforcement action if firms are working to the agreed roadmap. The roadmap predicts the number of declines transactions to be around 5% in June 2020 instead of the forecast 15% without an extension.

UK Finance is busy preparing a migration plan, which they refer to as a roadmap, and seeking FCA agreement. The plan includes several key metrics and milestones, which include customer readiness, merchant readiness and fraud reduction. The roadmap promotes two long-term strategic solutions. 1) an ‘Accessible Solution’ that uses OTP Authentication. 2) a ‘Strategic Solution’ using Biometric Authentication. The recommended Accessible solution can have an additional knowledge factor added during the course of the roadmap period if the fraud position changes negatively. The strategic biometric authentication solution is fully SCA compliant as the mobile device is an acceptable possession factor and inherence is provided through the verification of the captured biometric. The objective of inherence is to prove that the legitimate cardholder is initiating the transaction.

> “A ROADMAP AND ADDITIONAL TIME IS NEEDED TO ALLOW ALL STAKEHOLDERS TO BE READY AND AVOID UNINTENDED NEGATIVE CONSEQUENCES”
>
> - TRADE ASSOCIATION

Our current understanding is that 14th March 2021 will be the new UK date for active enforcement of SCA compliance but this has not yet been confirmed by the FCA. Some transactions may require SCA before this date and other more complex use cases may require longer. The expectation is that this roadmap will be formally agreed in August although the position may change once again. ■

7. Authorisation Strategies

Regulatory compliance is seen to be the highest priority for all issuers. Lack of compliance means they risk facing fines or even a loss of their operating licence. Our research showed that fraud prevention was their second highest priority. They are keen for fraud losses to reduce and recognise that action has to be taken (which may add pain) to achieve this objective.

The figure of £566 million of losses, and with this amount continuing to grow, is not sustainable in the long term. Operating in a highly competitive market and where customers often have payment cards from more than one provider customer experience is also a high, but not a top two, priority. New authentication methods, such as the greater use of biometrics, will help improve the UX but these are not expected to initially be available for implementation. Updated authorisation message specifications have been issued by the international payment schemes to include fields required to indicate SCA out of scope indicators, exemptions and step up authentication requests. UK Finance has similarly released an update to Standard 70.

> “IT IS GREAT TO SEE DEBIT CARD ISSUERS INTRODUCE FEATURES LIKE CARD FREEZE THAT WE HAVE OFFERED FOR YEARS”
>
> – PREPAID CARD ISSUER

Issuers know that customers will not be happy with some of the changes, as extra friction is being added, but expect them to adjust over time. Issuers are hoping that the decline in UX will be temporary and within one year they will have become familiar with the enhanced security processes.

Merchants will probably be unsurprised to learn that issuers rated the likely negative impact of SCA on merchants to be a lower priority. Acquirers will seek to reduce negative impact by maximising the use of SCA exemptions including TRA.

Our survey found that merchants are generally receiving a reliable online authorisation service with over 75% of issuers delivering greater than 99.99% (four nines) electronic authorisation availability over the last year, with 30% achieving an impressive 100%. At 99.99% an issuer will be unavailable to authorise transactions for less than 53 minutes in a year. Regulators recognise the importance of merchants receiving a reliable authorisation service as demonstrated by the recent fine of £1.89 million on one issuer that had an 8-hour outage impacting 3367 customers and 5356 transactions. Payments processing has become mission critical for most merchants today especially since the growth of online sales, which can be made 24x7x365. Issuers must be able to maintain and upgrade their authorisation systems without impacting merchants or consumers. Issuers wish to advise merchants that they are moving to an environment where all transactions will need to be authorised online.

> “THE MAJORITY OF OUR CUSTOMERS SHOULD ADJUST TO THE NEW SECURITY PROCESSES WITHIN 3 MONTHS”
>
> – DEBIT CARD ISSUER

Recent card scheme mandates are forcing all contactless transactions online and offline transaction use cases are gradually being phased out. The case for shifting PIN verification online is another topic generating discussion this would help align the UK with continental Europe.

The main reasons for issuers declining transactions are insufficient funds, invalid card details/expired card, card having been reported as lost or stolen, suspect geographic location, an address verification service (AVS) mismatch, exceeding transaction limits or unusual transactional behaviour. Soon to be added to this list will be the lack of customer authentication. We heard that 70% of UK issuers expect to decline direct to authorisation transactions without an authentication or exemption.

Many issuers are planning to provide cardholders with increased self-management control of their accounts. One of the most popular features is supporting a card freeze in cases where a cardholder has temporarily mislaid their card. This can prevent the pain and cost of reissuing a card unnecessarily and the need for the customer to update payment records with multiple parties. Restrictions on channel usage, like no ECommerce or ATM transactions, daily limits or country restrictions are features currently being considered by several issuers.

> "70% OF ISSUERS EXPECT TO DECLINE DIRECT TO AUTHORISATION TRANSACTIONS WITHOUT AN AUTHENTICATION OR EXEMPTION"
>
> - TRADE ASSOCIATION

A very high reason for fraud and transactions being declined relate to geographical location. The approach gaining higher popularity is to deliver realtime transaction notifications for each transaction, with clear instructions on how to report a suspicious transaction or attempted fraud.
Issuers are making greater usage of proactive telephone calls for suspicious transactions or sending out messages as SMS or within a banking app.

Issuers are paying greater attention to merchant category codes (MCC). They are blocking more high risk MCC completely (drugs, pharmacies, gambling, gaming, timeshare, adult, dating, ticketing, direct marketing, pay day loans, binary trading, funding platforms) and looking more carefully at sectors like airlines, travel operators, hotels and furniture retailers, where long delays exist between time of booking and goods being shipped as these create higher risks of chargebacks.

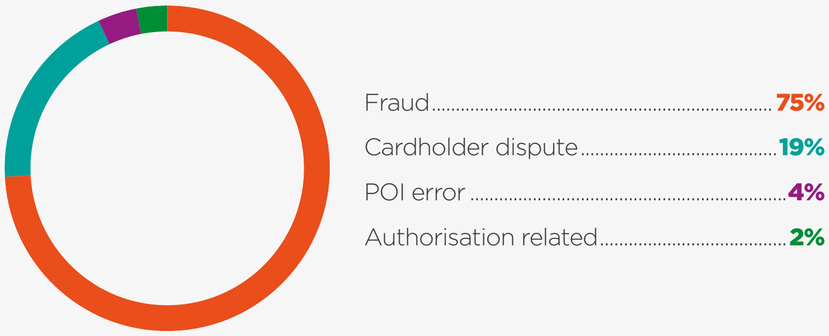
Issuers continue to suffer high fraud losses when a card is fraudulently used to fund digital wallets. Most issuers are operating automated fraud rules which block specific MCC codes and some merchants have also reported that since the need for refunds to be authorised online valid refund transactions are also being declined due to automated fraud rules blocking these transactions. It is therefore critical for merchants to ensure that the correct MCC classification is being applied. ■

8. Chargeback Disputes

The important thing to highlight when it comes to Chargeback disputes, is the growth in relation to eComm. With nearly 7% growth in Britain's online transactions (e.g., those made by card), chargeback rates have climbed from 11% to nearly 23% in the last 24 months. To consider chargebacks are 3Xs higher than the growth rate of transactions is an indicator of friendly fraud abuse.

Chargeback disputes can commonly be divided up into four main categories: fraud, cardholder dispute, point of interaction (POI) error, and authorisation related. The largest two are fraud, which accounts for 75% and cardholder disputes at 19%. We heard that friendly fraud is becoming an increasing problem.

Chargeback by category



The majority of issuers reported that the absolute number of chargeback disputes has stayed at around the same level as one year ago. 20% said that the number had increased but at a rate of less than 10%. We heard that interchange revenue reduction has impacted resource levels reducing effectiveness of handling disputes. The growing trend to outsource is reducing the amount of in-house specialist expertise.

> “A COLLABORATIVE APPROACH IS REQUIRED TO TACKLE FRAUD AND IMPROVE THE EFFICIENCY OF THE CHARGEBACK PROCESS”
>
> – ISSUER

When asked about the impact of the new Visa Claims Resolution programme, the feedback was generally positive.
The accuracy of claims appears to be improving and operational benefits are starting to be achieved. These include an average 15% reduction in the time to resolve disputes and more than 10% man hour savings. Of note however; is that the increased yield of efficiency has come with a price. According to Chargebacks911, the average chargeback filed per chargeback customer between 2017 and 2019 for the UK has climbed from 1.26 to 2.1. Reducing friction to improve the experience for the consumer is creating more dispute activity, not less. Many believe this is a primary catalyst for friendly fraud, as consumers are benefiting from near-instant gratification (i.e., receiving a refund) due to a much more automated approach. Simply stated, more than ever before; the responsibility lies on the acquirer and the merchant to proactively refute friendly fraud cases and provide issuers with a mechanism of defence.

We learnt from several of a poor VCR implementation process and that it is taking time to adjust business practices. The consensus view is that it is too early for findings on the impact of the VCR counterpart, Mastercard Dispute Resolution programme (MDRI). Issuers continue to encourage merchants to make customer service contact details more accessible and an increasing number of disputes have been seen if Payment Facilitators do not make descriptors (i.e., description of retailer name, product or store) clear on receipts and statements. ■

connect to address 192.168.1.1
username: #########
password: ###########
Access granted...
exited after 0.006146 seconds with return value
any key to continue

9. Recommendations for Merchants and Acquirers

Our discussions with issuers, acquirers and schemes have identified a number of clear recommendations for merchants. If these are followed then the amount of disruption to the payments experience can be reduced.

Ref	Activity	Recommendation
1	**Proactive Scheme Engagement**	Actively engage with collaboration tools offered by Visa (VMPI) and Mastercard's upcoming MDRI (Mastercard Dispute Resolution Initiative), which help combat fraud in realtime and maintain TRA exemptions. Greater dialogue between all stakeholders will help identify any issues and ensure answers are found. Using a partner facilitator may provide near immediate results, bypassing a lengthy technical integration. Chargeback reduction efforts have been noted up to 30% for high risk MCCs.
2	**3DS**	Implement 3DS technology as a priority. Don't be put off by poor feedback from early v1.0 implementations. Prepare to support v2.2 as early as possible with v2.1 as a practical interim step.
3	**MCC**	Ensure the correct MCC is being used for your business. Automated fraud rules are increasingly being used to decline transactions from high-risk business types.
4	**Indicators/Flags**	Make sure you correctly flag transactions and apply the right indicators and exemption requests. This may also require support for updated authorisation message formats.
5	**Chargeback feedback**	Ensure there is active engagement and provide collaborative feedback through the use of representments and 3DS v2. Share more data elements to allow more informed risk decisions to be taken.
6	**Education**	Help in the task of communicating with customers for both remote purchases and in-store sales. Your help is also needed in training store employees in updated payment acceptance processes.
7	**Business practices**	Expect to make changes to some business practices. MIT exemptions can only be used if the customer has explicitly accepted payment terms.
8	**PED & POS**	Make sure all payment terminals are Chip & PIN compliant, have at least PTS v4 security certification and support updated authorisation message formats and new step-up authentication reason codes for contactless transactions.
9	**Complex use cases**	Help explain any complex use cases that may require further discussion. Collaborate to find appropriate solutions.
10	**3rd parties**	Review your current suppliers and confirm on-going suitability. Make sure your third party providers are aware of SCA implications and commit to delivering compliant services.

10. Conclusions

Payments processing is a mission critical service for most merchants today. A loss in revenue will be seen if customers abandon baskets, walk out of stores or decide not to return. Issuer strategies have a direct impact on merchants as any increase in friction or fraud controls has a negative effect on the payments experience and customers. Our research found that 58% of issuers felt that too much friction is being introduced. We learnt that merchants are generally receiving a strong electronic authorisation service with over 75% of issuers delivering greater than 99.99% availability.

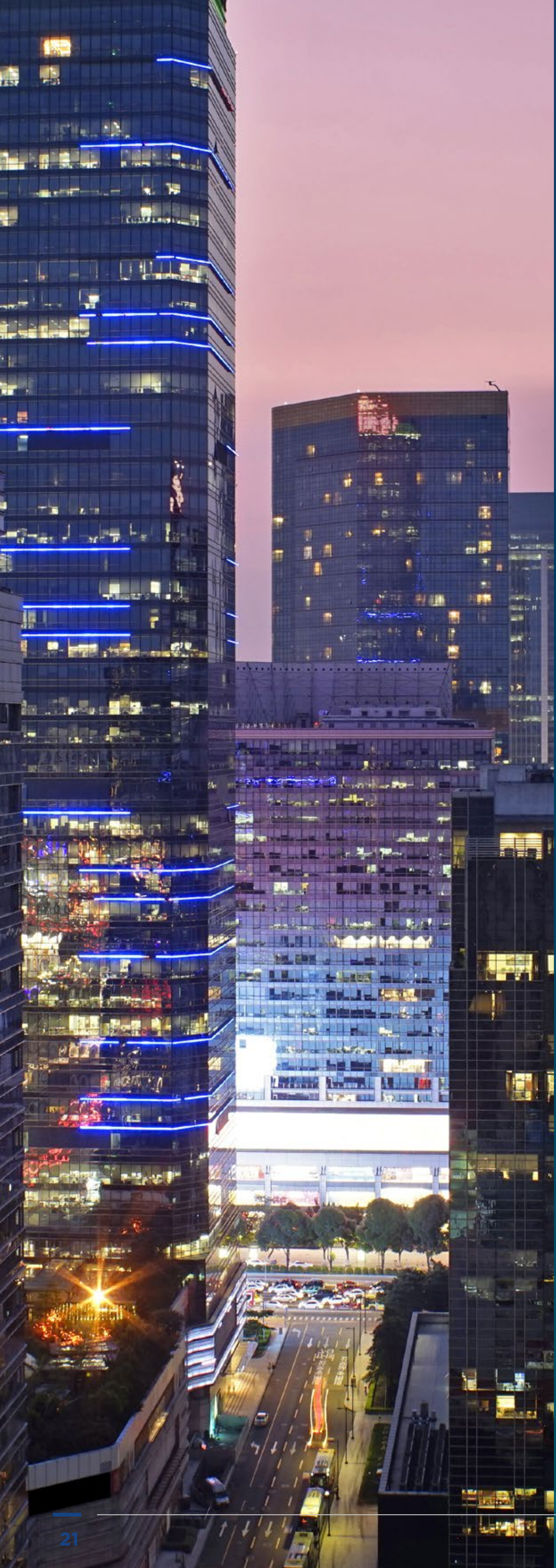
Escalating fraud levels remain an area of concern and particularly for remote purchases and eCommerce where annual losses now total £310 million out of the £566 million overall card fraud total. Regulators have determined that action has to be taken in order to reduce these figures and maintain consumer confidence. Most card transactions now need to be authorised online helping issuers identify fraudulent transactions through the use of advanced authorisation features, risk management systems and artificial intelligence tools. A greater focus on merchant category codes allows transactions from high-risk sectors to be declined. Issuers are also empowering customers to self manage their accounts through the delivery of realtime notifications and the ability to temporarily freeze a card or block higher risk channels or transaction types. The EBA has also recognised the epidemic of "friendly fraud", providing compliance relief to proactive acquirers and merchants, through TRA reporting allocation.

Strong Customer Authentication is being introduced as part of the PSD2 regulations and this will impact merchants. 74% of issuers expect SCA to lead initially to a decline in user experience. The research shows that between 30 and 50% of eCommerce transactions will in future face a step-up authentication request, up from the current 2% level and that issuers expect in the short term to decline between 25-30% of transactions unless a managed roadmap is agreed. The three key approaches issuers plan to use are 3DS v2 technology, OTP delivered by SMS and authentication within apps. The long-term strategic solution relies on the use of smartphones, mobile banking apps, biometrics and 3DS v2.2.

Our research found that 74% of issuers said they would be ready by the 14th September from a compliance standpoint, but that they would not be operationally ready. Over 50% would not be able support exemption requests and with none able to support white listing of trusted beneficiaries. They will likely not be ready for 3DS v2.2 until late 2019. Issuers are not the only payments industry stakeholders to be unprepared for the September deadline. Acquirers, gateways and merchants will largely also not be ready thanks to the short timescales, late confirmation of requirements, solution availability and lack of awareness.

A national roadmap to enforcement is currently under discussion (expected to be confirmed in August), which will provide a further 18 months before active enforcement starts and the need to decline any transactions without an authentication or exemption. This has not yet been agreed and so must be treated with caution. Merchants must use this extension wisely to adjust systems and business processes to become compliant. A key element will be the introduction of 3DS v2.1 and v2.2 technology, which should be implemented as quickly as possible. Merchants need to ensure card transactions are correctly flagged with the right indicators and exemptions being applied and ensure they share more data elements with the issuer.

Chargeback disputes are increasing, with fraud accounting for 75% of all disputes. Friendly fraud is the biggest area of concern for Merchants would like issuers to use the full range of decline codes when declining transactions. The Visa Claims Resolution programme is starting to achieve its objectives and delivering benefits but has been hampered by a poor implementation process and more time is required before a change in behaviour is seen. Viable strategies for both Acquirers and Merchants to help avoid chargebacks includes scheme initiated collaboration, such as VMPI and MDRI. Near immediate adoption may be achieved through a Programme Facilitator. ■



About Chargebacks911

Chargebacks911, also known as The Chargeback Company in Europe, provides cutting-edge, highly-scalable enterprise solutions and specialised consulting for chargeback compliance, risk mitigation, and dispute management to acquirers, card issuers, and merchants. The company's dynamic technologies and tactical data analysis help decrease the negative impacts of chargebacks and disputes, thereby increasing customer retention and revenues.

Chargebacks911 is recognised as the world's leading platform provider for comprehensive dispute mitigation and remediation technology. They are a certified VMPI Facilitator and support all major and minor card schemes, as well as the majority of European APMs. Chargebacks911 has been named "Best Chargeback Management Solution" for three consecutive years, and the company's patented technology was named "Product of the Year" for 2018.

Notes:

EMERGING PAYMENTS
ASSOCIATION

Emerging Payments Association
London, SE1 9SG, UK
Tel: +44 (0) 20 7378 9890
Web: emergingpayments.org
Email: info@emergingpayments.org
@EPAssoc
in Emerging Payments Association