PSD2 Strong Customer Authentication (SCA)

for the Travel & Hospitality sector

Elavon®

Let's get started

"Unintended consequences of the regulation" is sometimes the best way to describe the forced smiles, shoulder shrugs and the inevitable frustrations and sighs of resignation experienced by many in travel and hospitality, as this most impacted sector continues to adapt to the changes required for PSD2 SCA compliance.

The security requirements for compliance are the same for all merchants in all electronic payment channels. It has, however, proven to be a challenge for even the simplest payment systems, evidenced by the need for enforcement delays provided by the various regulators.

Implementing the more complex business, operational and technical changes required for the Travel and Hospitality (T&H) sector is proving to be even more challenging.

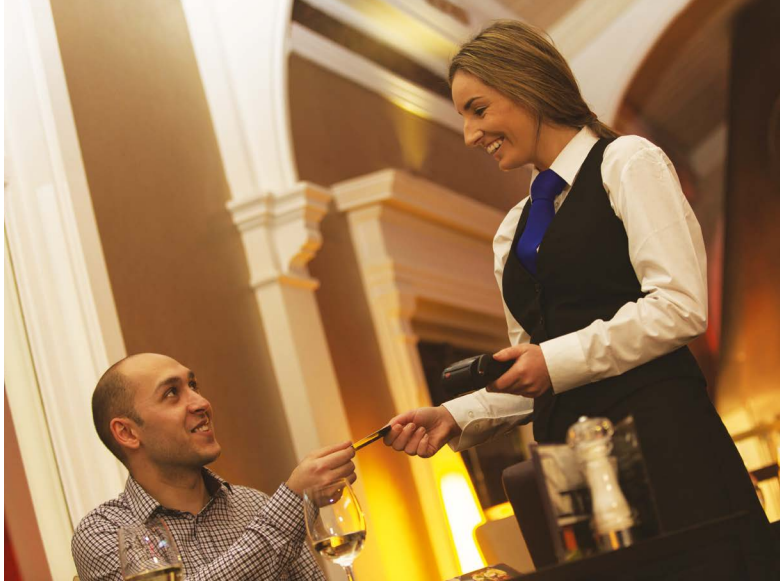
- In your direct sales eco-system you already have wide variety of 'online, in-app, in-store, on-board and on-site' payment devices and channels, often from an array of vendors and suppliers that will include Property Management Systems (PMS), Travel Management Systems (TMS), integrated and non-integrated point-of-sale system providers (POS and ePOS), websites and smartphone apps and others, all requiring your attention.

- In your indirect sales channels, things get even more complicated. Sales generated through independent third parties and booking agents where your first customer contact triggers a series of payment transactions (before, during and after customer visits) are all within scope. Booking and Travel Agents (OTA), Travel Management Companies (TMC), Corporate Booking Tools (CBT), Central Reservation Systems (CRS), Global Distribution Systems (GDS) and every other T&H merchant acting as an agent for another merchant or any market players involved in the booking process if they contribute to the processing of the payment transaction, must be engaged in SCA processing and upgraded for your compliance, as well as their own.

Elavon, together with the card schemes and other industry-wide stakeholders recognise the challenges remaining with some interpretations of the Regulatory Technical Standards, as well as a lack of industry-wide technical specifications and guidance available to address the upgrades required for such a fragmented, complex and far–reaching eco-system.

In recent weeks, some of the regulatory ambiguity has been cleared away and technical specifications are emerging to fully enable the European T&H payments infrastructure for compliance. Card scheme transaction frameworks have evolved to meet new requirements and although some pieces of the PSD2 SCA puzzle still remain unsolved, the direction of travel is clear for all and the implementation options have now been clearly defined for this complicated merchant sector.
We're going to explore those implementation options with you now so that you can better decide:

- How you continue or modify your engagements with your customers on first contact.
- How you establish transaction processing procedures with your customers and indirect sales channels via consents and permissions supported by T&C agreements.
- How you will balance the desire for frictionless flows with the risk of liability shifts that will result from your decisions on your preferred options.



All T&H merchants strive for and rely upon a smooth customer journey. That starts with the first contact and continues throughout the experience until that customer returns home again safely.

At Elavon, we want that same service ethos for your payments processing. Safe and secure transaction journeys with frictionless flows, from start to finish.

If you want to ensure that you achieve and maintain compliance with the regulations and continue to provide frictionless payment processing for your customers, the following will provide you with some valuable insights. You'll be pleased to learn that those 'unintended consequences' of the regulations for your complex customer payments are all being dealt with.

Which Travel & Hospitality transactions are in scope of the regulations?

All of them. Unless exempted from SCA by the Issuer or Acquirer (the regulated entities), or unless the transaction is identified and flagged as Out Of Scope, all electronic payments in all of your direct and indirect sale channels must be securely authenticated.

Failure to secure your payment channels with SCA, or failure to correctly flag for SCA exemption requests, or failure to flag correctly as Out Of Scope will result in transaction friction and failure for your cardholder payments. Together with the shopping cart abandonment that often accompanies the introduction of payments friction, you can expect to receive authentication step-ups when you are unable to deal with them, leading to unnecessary transaction declines, reductions in approval rates and ultimately lost sales.

Transactions exempt from SCA – few for Travel & Hospitality

There are transaction based and risk based exemptions available to SCA, and some of these require agreement with your payment service provider and acquirer before they can apply.

In the category of transaction based exemptions we can find contactless, recurring, low value and unattended transport and parking transactions, most of which will be of limited use to you. More widely relevant will be Trusted Beneficiaries and Secure Corporate Payment exemptions, both of which have merit and will enable frictionless flows but also have their limitations in terms of scope and guaranteed availability for all of your customer segments. Despite any drawbacks, these are important exemptions types so we will cover these in detail for you in a later update.

The only other exemption types left for the sector to take advantage of are risk based exemptions applied by either the issuer or acquirer based on their fraud risk analysis of the transaction as it takes place in real time.

When applied for and accepted, these Transaction Risk Analysis (TRA) exemptions will result in frictionless flow however they have restrictive limits imposed on them. Predicated on existing fraud ratios across the eco-system being managed to tight tolerances, by definition these transactions must be systematically identified as 'low risk'.

They come with transaction value limitations which will render them irrelevant to all but the smallest of merchants. The average transaction value of payments in this sector far exceeds the transaction amount thresholds permitted by the regulator, so expect to find these exemptions types will be of limited use to you.

The restrictions and limitations placed on exemption types by the regulators leaves few exemption possibilities for the T&H industry. This means that most of your payment transactions will require SCA and the potential for friction that comes with it, unless they can be considered Out of Scope.

Transactions out of scope for SCA – key for Travel & Hospitality

In a previous update we described Cardholder Initiated Transactions (CIT) and the general PSD2 SCA principle that because the cardholder is 'in-session' ('in-store' or 'online) and capable of being authenticated, then they must authenticate. This applies even if the cardholder is paying with previously stored credentials (COF).

However, by legal necessity and for implementation practicality, some transaction types have been considered Out of Scope of the SCA requirement.

One Leg Out (OLO)

If either the issuer or acquirer is outside of the EEA/UK legal jurisdiction then SCA need only be applied on a 'best efforts' basis. Authentication may or may not be possible depending on the SCA readiness of the unregulated leg.

Mail Order/Telephone Order (MOTO)

For genuine MOTO transactions, the cardholder cannot be authenticated.

Anonymous

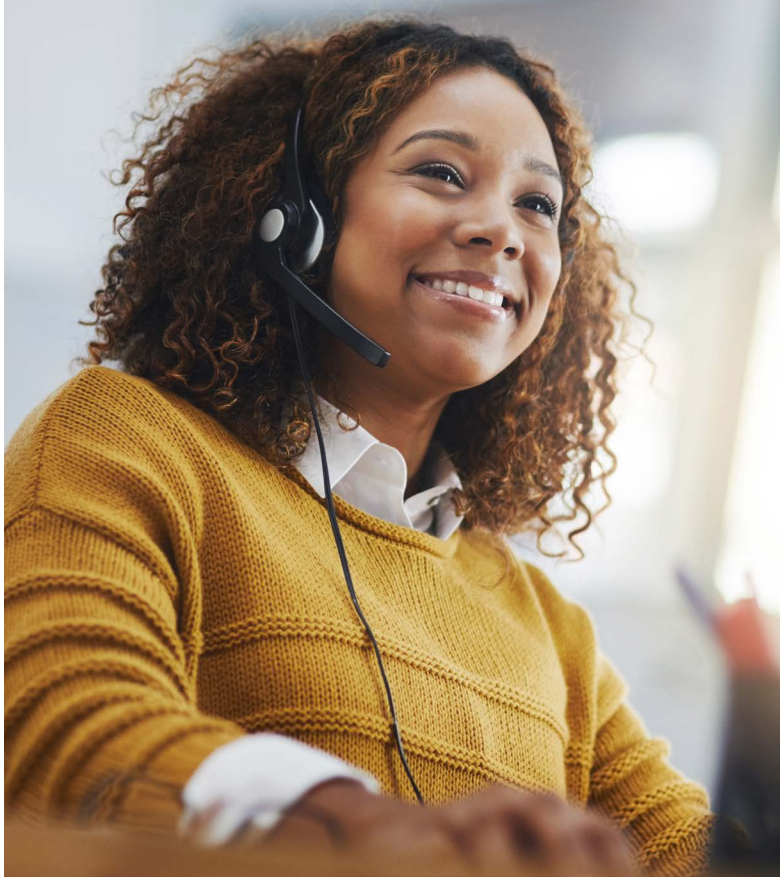
If the cardholder cannot be identified from the payment instrument, it stands to reason that they cannot be authenticated. (e.g. anonymous pre-paid cards).

Merchant Initiated Transactions (MIT)

A merchant initiating a transaction with the cardholder's prior agreement but without the cardholder present or 'in-session'. Cardholder cannot be authenticated.

These all have relevance to the T&H sector however MOTO and MIT transaction types in particular are mission-critical and common features of the T&H payments landscape. Accurate use of both will be key to your success in reducing payment friction.

MOTO – Mail Order/ Telephone Order transactions



These transaction types can only be initiated by telephone or mail. They remain Out of Scope and require no authentication. Note that manually key entered transactions into an electronic device are still permissible for MOTO flagging provided that the cardholder is not present and the transaction originated in the mail or telephone channel. Manually key entered transactions are not permitted when the cardholder is present (in-session) and these must be authenticated, and not flagged as MOTO which has historically been a common industry practice.

As per key PSD2 SCA principles, the cardholder is not 'in-session', cannot be authenticated, issuer approvals will shift fraud liability towards you. Frictionless flow results.

MIT – Merchant Initiated Transactions

MITs are transactions governed by an agreement between the merchant and cardholder which allow you to initiate subsequent payments from the card without direct cardholder involvement. The terms and conditions of the agreement must be clearly disclosed to the cardholder and SCA must be performed on the first transaction in the series when setting up the MIT agreement.

As per key PSD2 SCA principles, the cardholder is not 'in-session', cannot be authenticated again in real time, issuer approvals will shift fraud liability towards you. Frictionless flow results.

MIT transactions enable you to perform payment transactions for a variety of scenarios where the cardholder is no longer available to be authenticated.

- Paying an initial balance or instalments prior to check-in or pick-up
- Blocking additional funds during a stay or rental extension
- Express check-outs and returns
- No shows and cancellation fees
- Additional or delayed charges for upgrades, fees, fines and damages

Remember that MIT (and MOTO) transactions must be flagged correctly to ensure that Issuers recognise them as being Out of Scope and do not challenge for SCA when the cardholder is not present and unable to authenticate. Correct transaction flags will prevent these transactions being 'stepped-up' and subsequently declined due to no cardholder response.

For MITs, the results of an initial SCA performed when setting up the agreement need to be referenced for each subsequent MIT. This authentication result 'payload' is referred to as 'proof of authentication' and its requirement in MITs causes some considerable challenges for T&H. In order to understand why it so important and what you need to do about it, you first need to understand just a little about the contents of the authentication result.

Cardholder authentication using SCA

Proof of authentication

Prior to any issuer being able to authorise a payment card transaction, they must be assured that the cardholder has been authenticated using SCA. This authentication might be taking place in real time as a one-off transaction is generated or the authentication might have taken place previously and the issuer is being asked to approve a transaction which is part of a pre-approved series.

Either way, the issuer must be advised that authentication has taken place and you do this by providing them with 'proof of authentication'.

Unlike a typical authorisation response code which is a simple string of digits that can be readily key entered into payment systems by operators, the results of an authentication request is a much more complex payload, elements of which will need to be extracted, stored and appended to subsequent transactions and due to the complexity of the payload, is not suitable for manual manipulation or operator intervention. The elements required for re-use will depend upon the transaction type being performed and the sequence of the transaction when it is part of a series. We will talk to that in more detail later when we introduce the technical specification for data transfer between third party booking agents and the merchant.

Moving the required data elements around within your direct sales infrastructure will prove simpler than within the indirect channels which traditionally lack the links and system integrations with you to perform such data transfers.

The issuer-generated authentication result contains key data elements for your re-use, and will be slightly different for each card scheme, but all follow the same logic and construct.

- A unique transaction identifier – a simple string of digits uniquely identifying this transaction.
- ECI – is an electronic commerce indicator that determines where the issuer has shifted liability.
- CAVV cryptogram – for card based transactions, a secure cryptogram is generated. These complex elements can be moved around through integrated systems but will prevent manual operator actions being taken. For example, an operator cannot manually key enter a cryptogram payload into a POS terminal. In the case of transactions performed under Chip & PIN/Contactless, these processes already take place automatically within the terminal and card interaction behind the scenes. That same level of security is now being applied to eCommerce transactions but due to the fact that the authentication result can be used for multiple transactions, these date elements need to be manipulated within your eCommerce transaction flows.

The 'proof of authentication' is now a critical part of the eCommerce payments processing chain and the ability to transfer it between players in the eco-system is a necessity, however for the T&H sector in particular, it presents some significant challenges for you which we will now explore.

Incorporating SCA into your direct and indirect sales channels

For your direct channels, the implementation approach and options are the same as for any merchant type. You must secure your physical and eCommerce card acceptance processes so that SCA can be performed prior to authorisation processing. For your physical devices this means EMV Chip & PIN/Contactless must be deployed across your entire estate. For your remote channels, the latest available version of EMV 3DS will need to be deployed.

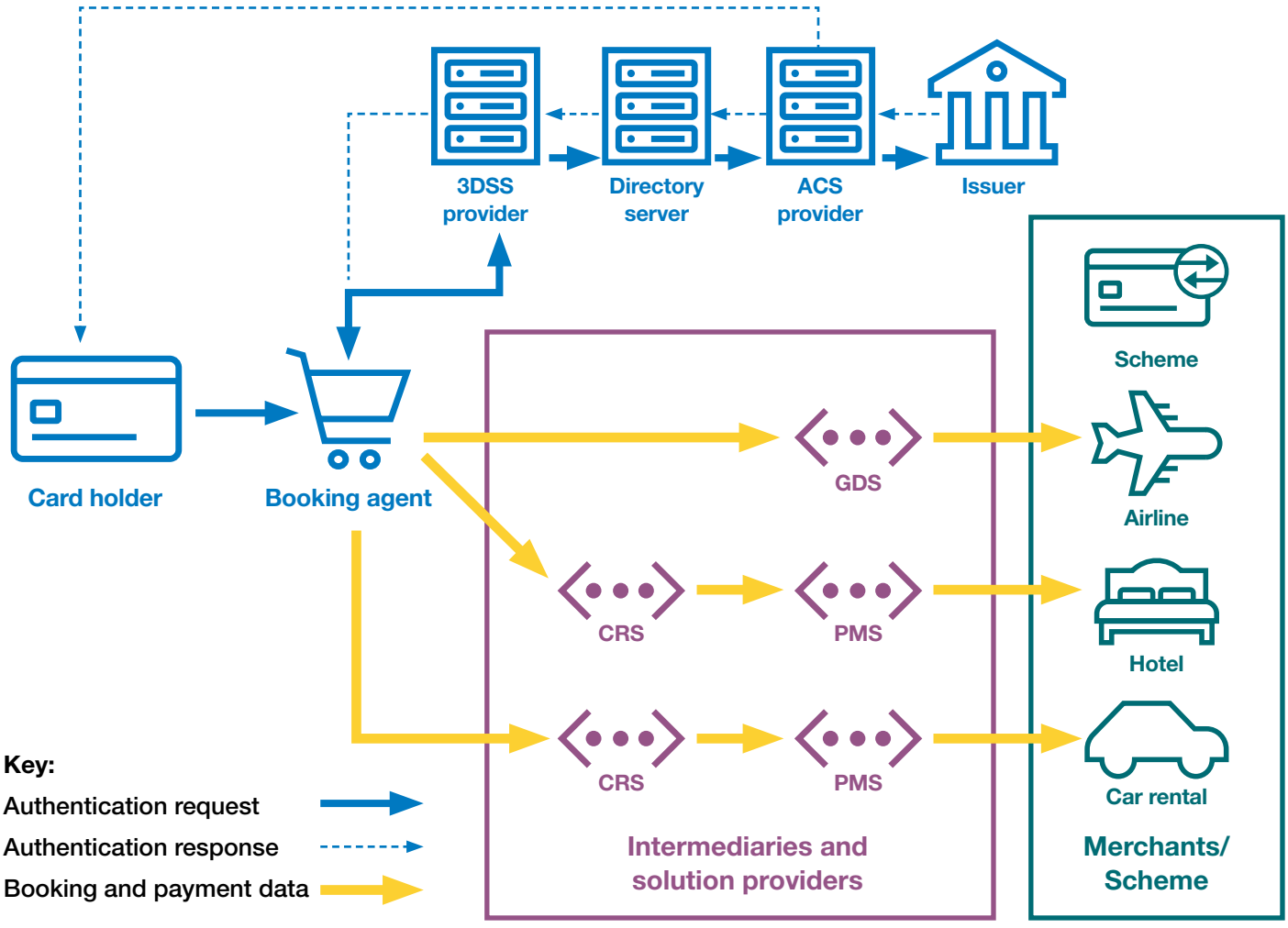
EMV 3DS will be used to:

- Authenticate the cardholder using two of the three possible factors determined by their card issuer. You have no control over which factors are used by the cardholder's bank to perform authentication so each cardholder's authentication experience might be different. Some will be asked to respond by entering a one-time passcode issued to their smartphone, others will be asked to respond with a fingerprint. There are multiple authentication options already and these will continue to expand as biometrics and other authentication techniques evolve and emerge. It's important to note that the cardholder will already be quite familiar and comfortable with the authentication factors chosen by their bank as that experience is consistent for them everywhere. By deploying the latest version of EMV 3DS, you are providing the 'secure pipes' for these cardholder to issuer bank interactions to operate through seamlessly, whatever the authentication factors chosen.
- Create part of the authentication payload referenced earlier. You will be capturing some data elements of the authentication response to create 'proof of authentication' for use in future transactions. The issuer's response at this point will also indicate where the liability sits in the event of fraud on this transaction.
- Flag for any permitted exemptions and ask for no step-up to SCA challenges in pursuit of frictionless flows.
- Enable cardholders to respond in a familiar and consistent way to step-up requests from issuers and acquirers. If either the Transaction Risk Analysis (TRA) at acquirer or TRA at issuer fails, this means a higher than expected risk has been detected and a step up to SCA must be completed.
- Allow you to request your own step-ups to SCA when a challenge is preferred. You may wish to do this to ensure full liability shift protection from potential chargebacks. There are also instances where you must obtain an authentication result and you do not want an exemption and frictionless flow granted by the issuer. For example, when setting up MIT agreements, SCA must be performed on the first transaction in the series so you don't want these transactions exempted.

For your indirect channels, your vendors, suppliers and third party agents providing you with bookings will need to make the same technology upgrades enabling EMV 3DS in their eCommerce channels however, the decision about who will actually process cardholder payments (agent or merchant) will determine how you incorporate SCA into your customer engagement strategy and approach to these channels.

Key principles of SCA in Travel & Hospitality transactions

- When a transaction is in scope of the regulations, authentication must take place at the time of booking in either the physical face-to-face environment via Chip & PIN or via EMV 3DS in the remote eCommerce channels.
- If the cardholder is not available at the time payment is taken, the transaction can be processed as MIT with the appropriate cardholder consents in place via T&Cs.
- The results of the booking agent's SCA process will need to be passed to the merchant processing the payments so that they can establish an MIT series for subsequent charges to the cardholder.
- The data elements to be passed between each player, (booking agent to merchant), will be determined by whether or not the booking agent is taking payments on your behalf (initial, partial or full payment) or whether or not all payments are to be processed by you as the merchant of record. In the latter case, the booking agent will perform just the SCA process and pass those results to you for subsequent payment processing.



Step 1

Authentication (and potentially an authorisation in some cases)

Step 2

Passing the authentication/ payment data between agent and merchant

Step 3

Authorisation by the Travel & Hospitality supplier

Indirect sales channels - options and impacts to consider

SCA must be performed on first contact at the time of booking with an independent third party agent. Determining who is going to accept and process card payments, a role that can be divided between you and your booking agents, is a key decision to be made which will impact all subsequent payment flows and cardholder interactions. Three primary options exist and for reasons of efficiency and ease of implementation you will most likely want to use the same adopted approach with each of your indirect channels. Variations of all three agent engagement models are in use today and can continue to be used provided that SCA processes are embedded where required by regulation.

Option 1

Agent has no 3DS SCA capability/agent takes no payments.

An unlikely scenario as most booking agents will be adopting EMV 3DS anyway, however this does closely mirror many present day agent-merchant relationships which you may which to continue. In this case the agent takes no payments. Payments are processed by the merchant directly after the booking event. The booking agent sends you the booking details as usual. However, for you to set up the MIT agreement, you will need to authenticate and authorise the cardholder yourself. This can be done via a 'pay by link' approach whereby a web address of yours is sent to the cardholder in an email (by you or the Agent) asking them to go 'in-session' to perform SCA on-line and consent to the MIT agreement.

This option might match your current agent arrangements and it requires the least amount of technical integration between the agent and you. The cardholder experience, however, is far from seamless as it introduces hand-offs and is reliant upon you reaching out to the cardholder via a link on second contact.

Option 2

Agent authenticates 3DS and collects all payments required on merchant's behalf.

In this scenario, the agent is 3DS enabled and performs the SCA process as well as authorising transactions and taking payment using the 'proof of authentication' they received. Merchant and agent T&Cs for the cardholder will need to be disclosed to, and agreed by the cardholder.

This option will also require payments to be made between the agent and merchant (agent has been accepting merchant payments on their behalf). These B2B payments can be achieved through any type of funds transfer mechanism, such as virtual cards, which can usually benefit from secure corporate exemptions, don't require SCA and can pass straight through to authorisation.

Note that if payments are taken by agents, and no MIT agreement is established, you will need a further customer interaction and SCA at check-in to cover for any potential additional charges.

Any subsequent MIT submitted by the merchant must contain 'proof of authentication' so merchant systems will need to be updated so that the transaction identifier of the transaction that contained the authentication value can be referenced. In this case the proof will need to come from the agent.

Option 3

Agent authenticates and all payments are to be processed by merchant

In this scenario, the agent is 3DS enabled and performs the SCA process on behalf of the merchant. For the merchant to be able to establish an MIT agreement and begin taking payments, the agent needs to pass the SCA results 'proof of authentication' to the merchant for use in its authorisations under the MIT framework.

Merchant and agent T&Cs for the cardholder will need to be disclosed to, and agreed by, the cardholder.

Note that the agent might take a deposit in this instance following the principles of Option 2 and performing some authorisation, however the collection of any remaining funds and any subsequent charges will need to be processed under MIT agreement by the merchant.

Summary of impacts to indirect channels

- Booking agents and any other indirect channels that you use should be upgrading to EMV 3DS as they must authenticate at the time of booking. If they cannot, then you must perform SCA on second contact using a 'pay by link' approach.
- Otherwise, booking agents should authenticate the booking as an MIT agreement on your behalf.
- Booking agents must clearly present T&Cs of the MIT agreement to the cardholder at the time of booking and prior to authentication.
- Merchants must update contractual agreements with booking agents to have them perform authentication and disclose MIT agreement T&Cs.
- Booking agents must pass to merchants (via any intermediaries) the 'proof of authentication' so that it can be used by the merchant for subsequent authorisations.
- An MIT indicator and reference to the authenticated transaction 'proof of authentication' must be present in any future authorisation requests and this impacts all payments including additional pre-authorisations during a stay or post event transactions like no shows.

There is something in the air – I think there is a gap

Now that we understand a little of what 'proof of authentication' contains, and we understand that for a merchant to process MIT transactions they must supplement each authorisation request with that 'proof of authentication', and that the proof required will vary depending on who initiates it and why, well then finally we can get to the core of the challenge facing the T&H sector.

We know that this is a highly complex eco-system comprising extensive legacy infrastructure, business models and service providers and intermediaries of all shapes and sizes. The heavy reliance upon indirect distributions channels makes their inclusion into the authentication process of paramount importance, however technical specifications to enable them to do that role do not exist, and many of the required 'linkages' between players either don't exist or are manual in their nature; we call these air-gaps. There are air-gaps in the required electronic flows within the infrastructure.

Somehow, the agent must pass the SCA authentication payload to the merchant via a complex and widely fragmented chain of intermediaries which prior to PSD2, had no need or desire to send complex data payloads (data fields, indicators and cryptographic data) between each other.

Until those essential technical specifications are published and the entire eco-system has upgraded to pass the authentication data 'proof of authentication' all of the way through the value chain from agent to merchant via its intermediaries, we will have a situation where SCA is actually being performed by the agent, an appropriate MIT agreement has been set up with the merchant however the merchant is unable to process those MIT transactions as the agents 'proof of authentication' cannot be sent.

Bridging the gap – a technical specification and guidance

Elavon has been working closely with regulators and card schemes across Europe, joining and driving think-tanks, working groups, task forces and other industry stakeholder groups dealing with these and the many other 'unintended consequences' of the regulation.

Although the UK, regulated by the Financial Conduct Authority, has agreed to an SCA enforcement date which is later than the rest of Europe, it was early to establish a national programme of works aimed at ensuring readiness and tasked with implementing a managed roll out. Those tasks were delegated to UK Finance which in turn established a T&H Task Force of subject matter experts and industry stakeholders to deal with the unique challenges of his sector. With the help of the card schemes, major global industry stakeholders and key industry technology suppliers, and all supported by Elavon, the task force accepted the mission of developing technical specifications and guidance for the industry.

The guidance and specification is now in draft form and is expected to be published late in Q3, 2020. Its objective is to inform agents, 'intermediaries' and merchants about what authentication and payment related data must be passed to merchants for their authorisation requests. The specification is valid across Europe and worldwide as many T&H suppliers are global. The guidance will specify which data elements must be passed from agent to merchant depending on which of the three options and scenarios you choose for engaging with your booking agents.

Bridging the gap – an interim solution only for Travel & Hospitality

Due to the late release of technical guidance and specifications required for the eco-system, and the length of time required for the industry to upgrade to the new specification via its many intermediaries, many merchants and agents will be caught out by the inability to process MIT without 'proof of authentication' and these transactions remain at risk of failure through declines. In summary, booking agents and merchants are not ready to pass the authentication data. Although an MIT with 'proof of authentication' is a best in class approach, it is very unlikely to be possible for December 2020 in the EEA and September 2021 for the UK.

Rather than have these transaction types fail and as a temporary measure, the card schemes are proposing an interim solution for regulator endorsement. Applicable to T&H merchants only and governed by a restricted list of Merchant Category Codes relevant to the sector, this aims to allow merchants to flag their MIT originating from indirect sales channels without 'proof of authentication' using existing Out of Scope flags.

Therefore for an interim period, and until such time as MIT with 'proof of authentication' can be provided with the new technical guidance, merchants will be expected to ensure proper use of either Out of Scope transactions types.

- Use the MOTO flag, and/or
- MIT flags to identify MIT transactions but with no 'proof of authentication'

Note that no additional flexibility is being sought to avoid SCA. SCA is required to be performed from the enforcement dates and must be performed at time of booking and when establishing MIT agreements. Flexibility is sought only for MITs that originate from third party bookings in the T&H sector – MIT without 'proof of authentication'.

Building the bridge – we all have roles to play

If you and your eco-system with its intermediaries and agents are able to develop to the new specification in time, then you should be looking to process MIT with 'proof of authentication' as a best in class and fully compliant solution, guaranteed to provide frictionless flow under the regulation.

Very few will be able to achieve that feat with such late notice and, as of yet, no guidance or technical specifications are available. Therefore the vast majority of the T&H industry will be relying upon the interim solution proposal of either MOTO or MIT without 'proof of authentication' accurately flagging these transactions as Out of Scope so that issuers know SCA challenges are not required.

Enabling the interim solution by bringing systems, process, procedure and policy into place ahead of the enforcement deadlines will require co-ordinated efforts and contributions from the entire industry.

Building the bridge – international card scheme actions

- Updates of rules and/or specifications as appropriate to include all merchant, acquirer and issuer interim solution requirements. Include key messages for Issuers and Merchants.
- Issuers must be aware that for an interim period, MIT transactions from T&H merchants that are the results of bookings made via third parties will NOT be able to bear 'proof of authentication' due to eco-system upgrade requirements for these merchants.
- Merchants must be aware that authorisation approval rates for transactions flagged as MOTO or MIT without 'proof of authentication' may be lower than transactions flagged MIT with 'proof of authentication'. Merchants should ensure they provide 'proof of authentication' as soon as they can.
- Incentivise the T&H industry to adopt the ultimate solution enabling 'proof of authentication' at the time of MIT agreement set-up.

Building the bridge – acquirer and issuer actions

- Acquirers will be updating contractual agreements with T&H merchants to confirm the requirements of setting up and executing upon MIT agreement for the interim.
- Acquirers will be putting controls in place to ensure proper use of the MOTO and MIT flags, ensuring that the requirements and conditions of MIT agreements have been met for transactions flagged as MIT without 'proof of authentication'.
- Issuers must not systematically decline MOTO transactions and MIT transactions that are sent without 'proof of authentication' from T&H merchants. Issuers must apply regular risk based assessment (RBA) for approving or declining these transactions.

Building the bridge – merchant and agent action

- Accelerate your efforts to secure all of your direct sales channels for SCA using both EMV Chip & PIN/ Contactless for card present, and EMV 3DS for eCommerce. Get to V2.2 as soon as possible.
- Decide on your customer engagement strategy and approach to SCA with your booking agents based on the generic options listed earlier – indirect sales channels – and advise your supplier and provider chain accordingly. Reach alignment with all third parties.
- Ensure that you plan to correctly and accurately flag your transactions according to the operating framework that you agree to with your booking agents in the above.
- Update your contracts with payment gateways and your acquirers for the right to use the MOTO flag or MIT without 'proof of authentication' if required for interim.
- Update your contracts with booking agents based on your decisions above.
  - Enable them to perform authentication on your behalf
  - Ensure that the terms and conditions disclosed at booking by agent reflect that cardholder is setting up MIT agreement with you, the merchant of record.
- Update your registration T&Cs at check-in to include MIT (in-app, front desk) to cover delayed charges and damages.
- Continue to communicate and align closely with your payment service provider (PSP), payment gateway partners and acquirers to ensure that any intermediaries in the chain are updated to pass the required data for direct and indirect processing pathways.

More to come

We hope you can see that a lot has been happening behind the scenes in support of getting your industry category ready to deal with the 'unintended consequences' of the regulations. Long awaited technical specifications are about to be released to enable full compliance for you and your third parties and, in the meanwhile, actions are underway to finalise the interim solution to enable us to bridge the gap until all upgrades are completed.

In later updates we will cover the other SCA exemption possibilities available to you including more on acquirer Transaction Risk Analysis (TRA) and the issuer exemptions of Trusted Beneficiaries and Secure Corporate Payments, all of which can help to offer your customers frictionless payment experiences.

Much more is still to be done and plans are well underway but right now your attention and focus is required on making those key SCA decisions for your indirect channel to enable the contractual, operational and technical changes to be ready on time.

Speak to your Relationship Manager for more details.

Elavon

UK 0345 850 0195 | **IRE** 1850 202 120 elavon.co.uk/PSD2 | elavon.ie/PSD2

Y3874V10820