PSD2 Review: SCA

Mastercard position paper on fraud and Strong Customer Authentication in the context of the PSD2 review

The revised Payment Services Directive (PSD2) has been instrumental in creating a new framework and rules for safety and security of electronic payments in the European Union. This has been a necessary and important development as the share of electronic payments continues to rise across all European economies. Both the proliferation of electronic payments, and the emergence of new technologies necessarily bring about new risks and threats, especially in the e-commerce space.

Mastercard welcomes the European Commission's initiative to create a more secure electronic payment ecosystem as corroborated by our existing efforts and central role in enabling and facilitating the industry's compliance with the new rules. We have advocated not only for mere compliance, but also the adoption of most innovative and best-in-class solutions while keeping a keen focus on user experience and future proofness.

Such efforts have required an unprecedented engagement by all relevant stakeholders to adopt and comply with the rules on Strong Customer Authentication (SCA), and although most of the industry has successfully adopted the new rules, many challenges remain.

In this position paper Mastercard outlines its views on key topics and issues, which in our view need to be addressed by policy and regulation to improve and fine-tune the system in place.

For any questions and comments, please reach out to Boris Martinovic at boris.martinovic@mastercard.com

***

Summary of Mastercard's recommendations

1. **New types of fraud**: To further improve the industry's resilience against fraud and to address new and sophisticated types of fraud, new measures should be developed, and consumer protection should be reinforced. A key measure would be to recognize behaviour-based information and characteristics, such as the EMV 3DS data, as a valid inherence factor.
2. **Exemptions**: The industry experience with SCA and exemptions suggests that the current exemptions regime should be fine-tuned for greater efficiency, user experience and balance. To this end, Mastercard suggests to:
    - address the travel industry issues, but also require compliance and monitor illegal use of exemptions;
    - recognize all MOTO transactions (including card-based MOTO) as out of scope;
    - extend the transport and parking exemption to electric vehicle charging and alternative fuel filling;
    - introduce a new exemption for vending machines and donation terminals;
    - raise the cumulative contactless limit for transactions without SCA to EUR 250;
    - introduce a new exemption for airline in-flight transactions;
    - extend the exemption under Article 17 RTS to all forms of access to corporate accounts.
3. **Liability**: Future regulation should recognize and define cases and instances of fraud where consumers should partially or entirely bear the responsibility.
4. **Level playing field**: To ensure level playing field between Merchant Initiated Transactions (MITs) and direct debits, SCA should be required for all mandates, including direct debit mandates.
5. **Internet of Things (IoT)**: Innovative solutions are bringing new forms of payment, including Autonomous (device-initiated) IoT transactions. To be future-proof and facilitate innovation and implementation of new forms of payment with an adequate balance of security and user experience, for specific use-cases, the new regulation needs to address device authentication as an enhancement for, or replacement of, consumer authentication.
6. **Hybrid cards**: PSD should allow the existence of hybrid cards which provide an open-loop and a closed-loop functionality at the same time, as these are innovative, already existing products with real consumer and merchant value. Instead of a blanket prohibition, the regulatory framework should rather address the specific safety and consumer protection concerns, if any.
7. **Business continuity**: The need to ensure business continuity during technical incidents should be addressed by the regulation, and in particular, future regulation should expressly allow payments without SCA during technical incidents affecting the SCA infrastructure.

8. **Compliance**: To ensure better compliance with SCA requirements, especially on the acquiring side, there should be more regulatory scrutiny of the acquiring/merchant community. In addition, to facilitate compliance with and implementation of TRA exemptions, the new regulatory framework should provide more and more practical guidance on how to properly perform the required audit of the TRA solutions.
9. **Transaction Risk Monitoring (TRM)**: The PSD2 review should address TRM with the aim of providing more detail and better definitions on risk monitoring requirements and data to be shared. We believe that an approach focusing on a minimal set of required data could help all parties in better risk analysis/monitoring. In practice, future regulation should force merchants/acquirers to share data with issuers, including personal data, in order to facilitate TRM and improve the overall effectiveness of the SCA regime.
10. **Card digitization in device wallets**: Card provisioning process through SCA factors that are provided and controlled only by the wallet provider is not compliant with the RTS, and the regulators shall take action in order to ensure full compliance with the regulation.
11. **Token issuance and replacement**: Regulators should answer / address the open question of SCA for issuance of tokens, and Mastercard is of the view that SCA should not be required for issuing tokens or updating them as long as this process happens in the background without the payer's intervention. This is because such issuance/update of the token would not qualify as an action 'by the payer' within the meaning of Article 97(1)© PSD2.
12. **Delegation and outsourcing**: As there is still uncertainty within the industry on whether SCA delegation qualifies as 'outsourcing' under PSD2 the regulatory framework should provide clarity on whether SCA delegation is outsourcing and clarify that, in any event, SCA delegation is not 'critical' outsourcing (which is subject to more stringent requirements under the EBA Guidelines on outsourcing).
13. **GDPR and behavioral biometrics**: The PSD2 revision should help secure a better legal ground for the processing of behavioral biometric data for SCA

***

1. Scope of regulation

1.1. New types of fraud

The new PSD2 SCA rules significantly contributed to reduce fraud rates in Europe, as shown by the below industry-level, relative figures, with Q4 of 2017 representing 100%:

	Q4 2017	Q4 2018	Q4 2019	Q4 2020	Q4 2021
Card present	100%	103%	68%	39%	50%
Card not present	100%	104%	79%	66%	46%

There is still room for improvement in combatting frauds however, especially in the e-commerce environment.

First, it is important that future regulation identifies and addresses new and sophisticated types of frauds, which are on the rising. Some of these are:

- Social engineering/phishing, whereby a fraudster steals credentials to initiate fraudulent transactions, and social engineering whereby fraudsters make cardholders authenticate the transaction.
- Consumer scams, whereby a genuine consumer is manipulated to make payments to a fraudulent payee.
- Account Data Compromise whereby the merchant/service provider's systems are hacked.
- Fraudulent refunds, whereby a fraudster uses compromised merchant credentials (or terminal cloning) to trigger fraudulent refunds.
- Technical weaknesses and/or incorrect implementation of SCA solutions.
- Card/account range testing on authorization/authentication infrastructure.
- Denial of Service attacks against authentication infrastructure
- Promo fraud type of attacks where fraudsters use multiple promotional offers by changing IP addresses and user credentials.

Second, future regulation may want to contain new measures to combat these new types of frauds:

- Consumer and merchant education is certainly key to raise awareness against new types of frauds and help consumers adopt secure behaviors when shopping online. Similarly, consumers should be educated on how to recognize scams including investment scams. Merchants (especially crypto wallets used by fraudsters) can play an important role and could be held liable if they do not sufficiently protect the consumer and block known 3rd party fraudsters (e.g. reported by several fraud victims) using their platform.
- Require wallets and similar platforms to offer consumers a mechanism for reporting scams and fraudulent 3rd parties using these wallets and platforms which should be obliged to

investigate these, maintain list of confirmed fraudsters and block them from service (for example based on blockchain address).

- Build a European database with identified fraudsters (including their names, addresses, blockchain addresses).
- Explicitly require payment gateways to use SCA for merchants to trigger payments, in cases where merchants are acting in their capacity as payers (e.g. refunds or to protect against transactions to test card credentials i.e. so called BIN attacks).
- EMV 3DS may also help reduce frauds, like phishing and scams, which cannot be prevented through traditional SCA methods. EMV 3DS provides extensive payment pattern information uniquely identifying the cardholder (e.g., spending habits, transaction history, location, device). With its more than 130 data points, EMV 3DS is more difficult for a fraudster to steal/compromise than individual SCA factors like SMS OTP or passwords. Importantly, the UK FCA recently expressly recognized that 'shopping patterns' may qualify as a valid inherence factor.

  It is namely the second factor (for example static password) that generates most of the declined transactions, because of poor user experience, also static passwords can easily be guessed by fraudsters and SMS OTP can be captured. EMV 3DS data has been already in use by Issuers for transaction risk monitoring and risk analysis for the TRA exemption to make low risk decisions and detect cardholders via their device/IP address and spending pattern. In addition, in the UK, pilots have been successfully conducted utilizing 3DS data as second 'inherence' factor.

  Behavior-based biometrics (e.g., keystroke dynamics, typing cadence, device angle) has been recognized by the EBA as an acceptable inherence factor. We believe that behavior-based information and characteristics, such as the EMV 3DS data, should also be recognized as a valid inherence factor. We consider that inherence can be defined as a characteristic attributable to a person regardless of whether it relates to a physical property of the body (for example a fingerprint) or a behavioral characteristic (for example, detailed shopping patterns), meaning that a characteristic or set of characteristics can be inherence without it/them being biometrics. In our view, the processing of behavior-based information/characteristics do not require explicit consent under the GDPR, as it is not processing of 'biometric' data under Article 9 GDPR.

  These kind of solutions are on the rise, multiple technologies are already on the market. More specific rules and definitions could help PSPs to better approach these types of solutions, for example by defining additional requirements for minimum accuracy, minimum detection results, what kind of certification can be accepted. This way PSPs could ensure that the selected technology is trusted.

Third, regulators may consider reinforcing consumer protection for new types of frauds, like scams, for which consumers are generally not protected under the PSD2 rules. The UK PSR is consulting on making reimbursements mandatory for authorized push payment scams. The European Commission may consider including similar protection measures within its review of PSD2.

Mastercard recommendation:

To further improve the industry's resilience against fraud and to address new and sophisticated types of fraud, new measures should be developed, and consumer protection should be reinforced. A key measure would be to recognize behavior-based information and characteristics, such as the EMV 3DS data, as a valid inherence factor.

1.2. Exemptions

The RTSs boldly provide various exemptions from the full application of SCA rules for certain types of transactions. Since the adoption of the RTSs and their implementation, the industry has gained experience with some transaction types, which may require a fine-tuning of the existing exemptions regime.

Travel sector

One problematic set of transactions is that in the travel sector, where the complexity is causing delays in complying with the regulation. Currently there are no exemptions in place specifically for this sector, while the UK FCA has tolerated flagging as MOTO as a way to bridge the non-compliance period. Because travel payments often involve multiple processors and aggregators, making these transactions fully PSD2 compliant is taking longer than expected. Regulators shall address the issues of the travel sector, but also require and monitor full compliance with the rules.

MOTO transactions

Another set of transactions which requires attention are the MOTO transactions, where confusion has arisen whether MOTO is in or out of PSD2 scope. The issue should be addressed and clarified. Mastercard believes that MOTO should be out of scope.

We are aware that the EBA held in two Q&As on MOTO and PAN Key entry that card payments (including PAN key entry) qualify as 'electronic' transactions and cannot therefore benefit from the MOTO exclusion. We, however, disagree with the EBA's position for the following reasons:

- The MOTO exclusion was introduced in PSD2 (Recital 95) because of the technological challenges in authenticating when placing an order via phone or mail.
- The MOTO exclusion was introduced in PSD2 to take into account cards. If the MOTO exclusion does not apply to cards, it is unclear which transactions may benefit from this exclusion.
- The EBA's view is not in line with the consolidated industry's position that the MOTO exclusion covers card payments initiated through mail or telephone (e.g., see Section 2.10 of UKF Guidance on SCA).
- The EBA's position contradicts positions previously expressed by the EBA itself. The EBA already recognized that card payments may benefit from the MOTO exclusion (Question 272(2) of the EBA Feedback Table attached to the final draft RTS of February 2017).

Being based on these wrong premises, and being by nature non-binding, it is unclear how the EBA answers on MOTO and PAN key entry may have any application in the short-term. We believe that a sensible approach would be to exclude all MOTO (including card-based MOTO) from SCA requirements.

Alternative Fuel Filling

The payment transactions relating to alternative fuel filling should also be addressed when discussing exemptions.

The European Union is boldly moving towards a sustainable future, as envisioned in the "Green Deal", and outlined in the "Fit for 55" legislative package. It is a welcome and necessary move to secure the wellbeing of Europe's citizens, for the generations to come. A key component of Europe's sustainable future is e-mobility and alternative fuels in general, where the EU strives to replace fossil fuel powered vehicles with those running on electricity[1] and other alternatives. It is a groundbreaking endeavor that will require not only the proliferation of electric (and alternative) cars, but also the creation of a Union-wide network of charging infrastructure with as much standardization and interoperability as possible, to secure broad, easy, and inclusive access for all European citizens.

The charging/filling infrastructure has several components that work as either enablers of broad uptake of alternative mobility, or a bottleneck. One such component is payment. In its proposal on the Alternative Fuels Infrastructure Regulation, the European Commission recognizes the crucial role payments make in designing an inclusive European charging infrastructure. We welcome the Commission's proposal to make payment cards the minimum and mandatory standard of payment at public recharging stations. We strongly believe that only a pan-European, open-loop, card-based payment solution would work as a low-barrier, universal means of payment in Europe, which is also confirmed by the consumers. Survey[2] results show that 65% of consumers would prefer to pay for electric vehicle charging by physical debit or credit cards, compared to 33% by cash, and less than 13% for any other means of payment.[3]

Apart from being inclusive, other important aspects of payment for electric (and alternative) vehicle charging include speed and convenience. Mobility, per definition, is movement of people, to which the charging of vehicles is typically an unwelcome but necessary interruption. Therefore, consumers want to be able to charge/fill their cars and pay for this service as fast and seamlessly as they can, to then continue their trip. It is mostly for this reason that the EU rules on Strong Customer Authentication for electronic payments, as stipulated in the RTSs under PSD2, provide an

[1] Here we include battery electric vehicles and hydrogen fuel cell electric vehicles.
[2] Survey was commissioned by Mastercard, and carried out by FTI Consulting in the Summer of 2021, in 7 EU member states: Germany, France, Italy, Spain, Poland, Austria, and Sweden. In all countries a sample representative of the total population and a minimum of 1000 consumers was utilized.
[3] It was a multiple choice question: „*Which of the following methods of payment would you prefer to use when charging an electric vehicle (if available)? (Please select all that apply)*"

exemption from the SCA obligations for transport and parking fares at unattended terminals.[4] The EBA clarified in reply to one of our questions that this exemption does not cover EV charging transactions (even when the payment for EV charging includes a parking fee - see EBA Q&A 2020_5224).

Already today, most of the electric (alternative) vehicle charging stations function as unattended terminals, and the industry expects unattended recharging terminals to represent a significant portion of recharging stations in Europe also in the future. As the nature and environment of electric (alternative) vehicle charging transactions is very similar (and in some cases identical) to those of transport and parking transactions, it would both make economic and social sense, and ensure legal consistency, for electric vehicle charging and alternative fuel filling transactions at unattended terminals to benefit from the same exemption. Furthermore, such an exemption would reduce the cost of infrastructure as installation of PIN-pads would become obsolete, while the risk of fraud would not increase materially due to charging transactions typically being of low value. No evidence suggests that fraud increased for transport and parking transactions because of the SCA exemption, while it helped preserve a seamless flow of movement in all the relevant use cases, such as public transport fares, highway tolls, etc.

In addition, almost 60% of consumers believe that contactless card payment without the need for strong authentication is a safe and secure way of payment for electric vehicle charging, while only 13% disagree.[5]

Apart from the new infrastructure, an exemption from SCA would also be beneficial to the existing recharging infrastructure, where a contactless payment card terminal without a PIN-pad is already in place. Due to the SCA requirements namely, most of these terminals need to be replaced, which is expensive, requires significant time and investments (and ultimately results in an increased burden for taxpayers in case of terminals deployed by municipalities). Terminals that are not replaced are then incentivized to rather accept closed-loop cards instead of open-loop cards, as closed-loop cards are excluded from PSD2 under the 'limited network' exclusion (Article 3(k) PSD2). This leads to regulation actually pushing the industry towards a closed-loop, more fragmented solution, contrary to the goals of AFIR, and also to open-loop cards being discriminated against closed-loop cards.

For the above reasons, Mastercard proposes to amend the Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), in specific Article 12 of Chapter 3, to also include electronic payment transactions at unattended payment terminals for the purpose of paying for electric vehicle charging and alternative fuel filling service.

[4] Chapter 3, Article 12 of the RTSs.
[5] Question and results from the same survey as referenced in footnote No. 1 above.

Vending machines and donation terminals

The EBA has clarified that SCA is required for transactions at vending machines, unless an exemption applies. This means that if vending machines are not equipped with a PIN pad and therefore do not support SCA, the payer will be unable to complete the transaction (EBA's Q&As 2020_5288 and 2018_4057).

With its answers, the EBA also clarified that the exemption for transport and parking transactions at unattended terminals under Article 12 RTS does not apply to vending machines for food and beverages. Hence, vending machines should be equipped with PIN pad to ensure that SCA may be applied. The same applies to unattended donation terminals as well.

Mastercard believes, however, that it is disproportionate to request SCA for transactions of very low amounts at vending machines and donation terminals, and they should benefit of the same exemption as the unattended terminals for transport and parking. Fraud data do not suggest higher fraud rates for vending machines or donation terminals compared to transport and parking machines, while the average transaction value is lower both at vending machines and donation terminals.

In case of donation terminals, Mastercard suggests to also introduce an amount limitation under which SCA would not be required, in order to avoid misuse. A reasonable limit could be 50 euros, in line with the per transaction contactless limit.

Contactless limits

A key measure to combat fraud in the physical environment has been the introduction of per transaction and cumulative limits to contactless payments, where the former currently lies at EUR 50, while the latter at EUR 150.

The EBA clarified in its Q&A 2018_4225 that "*it is possible to make cumulative transactions above €150 under Article 11* […] *without the application of* […] *(SCA) if less than five transactions have been made after the last application of SCA*". It is therefore allowed to have a maximum of five consecutive transactions up to a cumulative amount of EUR 250 (i.e., five transactions of EUR 50 each).

To harmonize the legislation and to provide a level playing field for all PSPs irrespective of their chosen way of compliance with the contactless limit requirements (number of transactions versus cumulative value), Mastercard proposes to raise the cumulative limit to EUR 250. The overall risk and liability do not change on the basis of the number of transactions (five or more), provided that the EUR 250 limit is not exceeded. In accordance with PSD2, increasing the cumulative limit will not increase liabilities for cardholders. Card present transactions are already very secure. Their fraud level is about 1 bp and constantly decreasing.

The European Commission expressly indicated in its Retail Payments Strategy the review of the current contactless limits as one of the priorities for its review of the PSD2 (page 18).

Airline in-flight commerce

The challenge with airline onboard acceptance is that due to lack of internet connectivity, the only solution the industry can currently advocate is not to use contactless and instead do Chip & PIN transactions, which is considered a step backwards and goes against market trends.

There is an increasing trend of airlines/acquirers blocking issuers from being accepted onboard/in-flight due to low approval rates. While decline reasons vary, there are common themes that impact consumer preference and merchant write-off rates alike.

As deferred authorizations for airline in-flight transactions are not (by default) exempt from SCA, issuers have no choice but to decline contactless transactions where SCA counters have been exceeded and ask for the transaction to be stepped up.

Unlike ICC Risk management parameters, SCA counters are not currently maintained on the chip for these cannot be taken into the consideration by the terminal onboard.

Based on an analysis done by Mastercard on ~10 Airlines in January 2022, SCA declines represent ~3% of spend volume overall with an increasing tendency driven by the increasing adoption of contactless card payments overall.

In consideration of the nature of airline in-flight transactions (i.e. offline environment when goods are handed over) and SCA related declines representing an inherent write-off to the airline, regardless of the actual issuer decision would have been from a credit and/or risk decisioning perspective, we believe that there are good arguments for airline in-flight transactions to be exempt from SCA requirements.

Corporate payment processes

Mastercard suggests that an extension of the Article 17 *Secure corporate payment processes and protocols* exemption under the RTS be applied to the provision of access to account and Account Information Services in a corporate environment (beyond that which is specifically mentioned in Article 10 of the RTS and in Article 10a of the EBA's revised draft RTS), as a number of firms within industry undertake business models whereby they only service corporate customers or other regulated PSPs.

Mastercard recommendation:

The industry experience with SCA and exemptions suggests that the current exemptions regime should be fine-tuned for greater efficiency, user experience and balance. To this end, Mastercard suggests to:

- **address the travel industry issues, but also require compliance and monitor illegal use of exemptions;**
- **recognize all MOTO transactions (including card-based MOTO) as out of scope;**
- **extend the transport and parking exemption to electric vehicle charging and alternative fuel filling;**

- **introduce a new exemption for vending machines and donation terminals;**
- **raise the cumulative contactless limit for transactions without SCA to EUR 250;**
- **introduce a new exemption for airline in-flight transactions;**
- **extend the exemption under Article 17 RTS to all forms of access to corporate accounts.**

1.3. Liability

The rules on liability are putting a lot of pressure on PSPs, even in cases where they should not necessarily bear all responsibility for fraud. To address this, there should be a definition of gross negligence, with examples where consumers would be liable instead of the PSP (to keep a healthy balance between consumer protection but also protecting banks, as well as providing a level playing field across EEA) such as:

- sharing payment credentials including OTP with 3rd parties, allowing others to use one's device with their biometrics (e.g. fingerprint) enabled and stored in the device;
- payments where amount and merchant were displayed to consumer, e.g. during authentication, do not (fully) reflect the intended payment – this explicitly includes merchants whose name resembles known entities (e.g. tax office, police) which means that if in doubt consumers should check with the impersonated entity whether they actually requested the payment;
- high risk investments that were clearly indicated as such (with promised returns much higher than market rates) that were delivered but then lost their value.

Mastercard recommendation:

Future regulation should recognize and define cases and instances of fraud where consumers should partially or entirely bear the responsibility.

1.4. Level playing field between MIT and SDD

The EBA clarified through its Q&A tool that MIT and SDD are out of scope of SCA requirements as they are transactions 'initiated by the payee only'. SCA is only required for the initial MIT mandate as this is an "*action through a remote channel which may imply a risk of payment fraud or other abuses*", which requires SCA under Article 97(1)(c) PSD2 (Q&A 2018_4031).

However, according to the EC and EBA, SCA is not required for a direct debit mandate if given directly to the merchant, without the involvement of the bank (Q&A 2019_4664). SCA is only required if the payer sets up her/his direct debit through her/his bank (e.g., through home banking). In our view, this creates an uneven playing field between cards and SDD.

We therefore propose that SCA should be required for all mandates, including direct debit mandates.

Mastercard recommendation:

To ensure level playing field between MITs and direct debits, SCA should be required for all mandates, including direct debit mandates.

1.5. SCA for Internet of Things (IoT) transactions

In our view, current IoT transaction models for replenishment services (e.g., smart printers, fridges, coffee machines) may benefit from the MIT exclusion. In particular, we believe SCA is not required for a model whereby:

- the IoT device is registered in a replenishment service platform;
- the cardholder sets the parameters for the replenishments;
- the replenishment service platform automatically places an order when the IoT device signals that a replenishment is needed.

In the future, however, smart IoT devices will increasingly be capable of transacting autonomously, based on implicit consumer intention, rather than explicit consumer interaction. This new transaction model will present opportunities to the payment ecosystem. Payment authentication, in particular, will need to move from a consumer-centric model to one that incorporates the attributes of the transacting device. In this model, as the transaction typically happens in the background, the consumer does not actively trigger the payment and may be unavailable or technically unable to authenticate.

For some use-cases the current consumer-centric model can continue to be used for autonomous IoT transactions e.g., the consumer receives an 'out of band' authentication request whenever their device wishes to transact. However, for other use-cases, the rich availability and analysis of device data means that devices can be identified and authenticated to a high degree of accuracy, giving assurance to the card issuer that the transaction credentials really are coming from the correct device. In these cases, device authentication can enhance, and eventually replace, consumer authentication, leading to a streamlined and frictionless transaction which does not require consumer intervention.

Technologies and solutions exist today which can identify and authenticate devices to a high degree of accuracy by analyzing device attributes, connection information and other data. A framework where these, and other, solutions become 'certified authenticators' could pave the way for device authentication to be used in payment transactions as an inherence factor. For tokenized transactions this could provide a second factor, alongside the presence of a DSRP cryptogram.

In summary, certified and trusted device authenticators can play a role in the authentication of IoT devices and this authentication should be permitted as an additional factor under SCA requirements. This will allow the development of innovative IoT payment solutions that ensure a streamlined and frictionless UX.

Mastercard recommendation:

Innovative solutions are bringing new forms of payment, including Autonomous (device-initiated) IoT transactions. To be future-proof and facilitate innovation and implementation of new forms of payment with an adequate balance of security and user experience, for specific use-cases, the new regulation needs to address device authentication as an enhancement for, or replacement of, consumer authentication.

1.6. Interdiction of hybrid cards

In February 2022, the EBA published guidelines on the limited network exclusion under PSD2. Under this Guideline, a single card cannot accommodate simultaneously open-loop (regulated) and closed-loop (unregulated) payment instruments, impacting products like meal vouchers, retailer cards or petrol/T&E cards.

This provision is motivated by consumer protection principles: the EBA considers that such products are confusing for cardholders who do not realize that they do not have the same level of protection with unregulated payment instruments than with regulated ones.

Mastercard is of the view that instead of a mere interdiction, awareness among cardholders should be raised, improving the communication around hybrid payment instruments. There are many innovative hybrid card products already in the market, which provide real consumer value, and regulation should not prohibit such innovative products, but rather create a framework where these products can exist and continue to provide value to consumers and merchants alike, while at the same time being safe and secure.

The purpose of PSD2 is to foster innovation in payments while ensuring safe and secure transactions and forbidding hybrid cards clearly impairs this balance between innovation and security at the expense of cardholders who benefit from the convenience and ease-of-use of such products. Hybrid cards have been widely adopted by consumers who would not understand why these products are suddenly removed from the market without at least a grandfathering regime being put in place.

This measure also impacts European market players who've been using hybrid cards in different industries:

- meal vouchers and multi-benefits cards (e.g. Edenred, Up, Swile);
- retailer cards (e.g. Carrefour);
- petrol and T&E cards (e.g.Total).

The payments industry invested heavily in security over the past years. Today, the fraud levels for card-present transactions are historically low. We have not seen fraud or consumer protection issues related specifically to hybrid cards and there's therefore no real problem to be solved.

Mastercard recommendation:

PSD should allow the existence of hybrid cards which provide an open-loop and a closed-loop functionality at the same time, as these are innovative, already existing products with real consumer and merchant value. Instead of a blanket prohibition, the regulatory framework should rather address the specific safety and consumer protection concerns, if any.

2. Implementation & interpretation

2.1. Business continuity

The need to ensure business continuity during technical incidents should also be taken into account in the context of the PSD2 review. In particular, future regulation should expressly allow payments without SCA during technical incidents affecting the SCA infrastructure. Having a solid resilience plan is key to avoid massive declines and frauds during a technical outage.

Some countries, like France and UK have already adopted a resilience plan recommending issuers to continue to authorize non-3DS transactions during a technical incident. This would be allowed even when an SCA exemption is not applicable.

The UK industry implemented a resilience framework, by recommending the usage of schemes' resilience flags in case of major incidents on authentication infrastructure. Additional guidelines should be developed for continuous transaction monitoring and fraud screening, usage of stand-in solutions and specific multi-level controls for PSPs.

In particular, the UK industry implemented the following resilience rules and guidelines (Section 19 of UK Finance's Guidance on SCA):

- recommend the use of schemes' resilience flags in the case of major incidents affecting Issuer, ACS or Scheme / Directory Server;
- continue to apply transaction monitoring and fraud screening for all transactions;
- recommend the use of schemes' Authentication Stand-In protocols in case of technical failures affecting Merchant / Gateway 3DS systems;
- SCA should continue to be applied for other actions like setting up an initial MIT mandate or adding a 'card-on-file'.

The UK resilience framework relies on multi-level controls managed by issuers, acquirers and schemes:

- issuers. Issuers should continue to carry out real-time risk assessments of transactions and decline high-risk transactions;
- acquirers. Acquirers should monitor merchant use of the resilience framework and support merchant performance improvement;

- schemes. Scheme rules should set out further details and standardize implementation and use of the resilience framework, with monitoring of merchant usage through acquirers.

Banque de France has also adopted a resilience plan recommending that:

- issuers continue to authorize non-3DS transactions on a risk-assessment basis (also if an exemption is not applicable);
- issuers authenticate transactions through a one-factor fallback solution (e.g., SMS OTP only) if an SCA solution is not available;
- acquirers send transactions directly into authorization with a 'resilience' flag provided by card schemes.

We believe that the approach adopted in UK and France is proportionate. It guarantees continuity of payments to the benefit of cardholders and merchants, without materially increasing the risk of fraud for payments in Europe.

Mastercard recommendation:

The need to ensure business continuity during technical incidents should be addressed by the regulation, and in particular, future regulation should expressly allow payments without SCA during technical incidents affecting the SCA infrastructure.

2.2. Compliance

For SCA to work properly and transactions to be able to go through without technical or other obstacles, it is important not only for the issuing side of the value chain to be ready and compliant, but also the acquiring side (including the merchants themselves) to be ready and support the authentication flows and processes.

As of today, the industry is still witnessing a relevant disparity between the readiness of the issuing and the acquiring side, with acquirers and their merchants still lagging behind. Therefore, it is crucial that regulators / NCAs put pressure on the acquiring side, in order to facilitate full compliance. Acquirer and their merchants should not be allowed to present transactions without SCA and no exemption or exclusion to issuers. Currently only successful transactions are reported to NCAs (only fraud reporting provides more insights), and with closer regulatory attention/monitoring full PSD2 compliance could be reached.

When a PSP wants to apply TRA exemption RTS SCA requires that "the methodology, the model and the reported fraud rates" are audited by an independent external auditor who has the necessary IT and security expertise. PSPs are required to provide their reports to NCAs. Since SCA introduction we are witnessing that some PSPs are reluctant to use TRA because there is not enough guidance how to do such an audit. We think more/practical guidance would greatly help these PSPs by adding more definition about minimal audit requirements, procedures, acceptable methodology, scope, fraud rate calculation/reporting review.

Mastercard recommendation:

To ensure better compliance with SCA requirements, especially on the acquiring side, there should be more regulatory scrutiny of the acquiring/merchant community. In addition, to facilitate compliance with and implementation of TRA exemptions, the new regulatory framework should provide additional clarity coupled with practical guidance on how to properly perform the required audit of the TRA solutions.

2.3. Transaction Risk Monitoring

The RTSs are in their present form regulation too high-level on transaction risk monitoring requirements, which makes its implementation and application difficult.

The PSD2 review should address TRM with the aim of providing more detail and better definitions on risk monitoring requirements and data to be shared. In principle, the acquirers should send more data than what is currently required to better support risk analysis.

Card schemes are already mandating the minimal set of data provided by PSPs, but on regulatory level a common standard about what kind of data should be shared (device, app/browser environment, transaction type) would support transaction risk analysis more effectively.

There are certain data points which are key in supporting proper risk analysis and assisting issuers in risk decision making and monitoring. If these important elements are missing/not sent by the acquirers/merchants it can prevent issuers from applying and further expanding the usage of SCA exemptions, as these are key data elements to support certain issuer risk models.

We believe that an approach focusing on a minimal set of required data could help all parties in better risk analysis/monitoring. Our experience shows that the below data points are critical for proper issuer risk decisioning and monitoring:

- Accountholder/cardholder data: Account number, accountholder name, email address, home/mobile phone numbers, billing and/or shipping address
- Device information: IP address and device ID

Mastercard recommendation:

The PSD2 review should address TRM with the aim of providing more detail and better definitions on risk monitoring requirements and data to be shared. We believe that an approach focusing on a minimal set of required data could help all parties in better risk analysis/monitoring. In practice, future regulation should force merchants/acquirers to share data with issuers, including personal data, in order to facilitate TRM and improve the overall effectiveness of the SCA regime.

2.4. Card digitization in device wallets

Majority of mobile payment solutions are using device-based wallet solutions, provided by Apple, Google, Samsung etc. When a card is added to the wallet (called tokenization process), card issuers and wallet providers (Apple, Google, Samsung) are working together to authenticate and verify the cardholder using their fraud system and communicating with each other through card networks.

The initiation of card tokenization can be initiated from the wallet app (controlled by wallet provider) or from issuer banking app. When the wallet app is used for such initiation cardholder can be authenticated with a onetime password (sent in SMS). Current implementations are relying on onetime passwords and credentials required for the device (user account + password). Whenever the first payment transaction is initiated after the card has been added, SCA is always required (by using device biometrics).

EBA has, however, provided answers on this topic (e.g., its recent Q&A 2021_6141), clarifying that during tokenization SCA must be applied with factors verified by the card issuer bank or by applying delegated authentication by the wallet provider (which would be possible with an outsourcing agreement between the issuer and the wallet provider).

We believe that the EBA's position that card registration in a wallet solution requires SCA by the issuer is fully consistent with Article 24(2)(b) RTS, which expressly require SCA by the issuer for the initial association of security credentials to the user.

The idea is that only the issuer is in the position to initially associate SCA credentials to the legitimate cardholder. When the issuer initially identifies the cardholder, it will associate that identity with credentials (e.g., a SIM card with a mobile number). Clearly, that SIM card is provided by a third party (a telecom operator). What matters is an initial secure association by the issuer.

Each subsequent association of security credentials (including tokenized PANs) should also be controlled by the issuer. This is because the entire process of associating SCA credentials with the user is as strong as its weakest link. This is very clear in the RTS and the EBA's Q&A 2021_6141 reflects this principle.

We therefore believe that a card provisioning process through SCA factors that are provided and controlled only by the wallet provider is not compliant with the RTS. For example, Apple Pay's manual card provisioning whereby the user is authenticated through SMS OTP + wallet ID is in our view not compliant with the RTS.

Mastercard recommendation:

Card provisioning process through SCA factors that are provided and controlled only by the wallet provider is not compliant with the RTS, and the regulators shall take action in order to ensure full compliance with the regulation.

2.5. SCA for token issuance/replacement

The EBA has already recognized that tokens qualify as an authentication element of 'possession' ("*something only the user possesses*") under the PSD2 RTS (EBA's Q&A 2019_4827 and Opinion of June 2019).

A question on whether SCA is required for the issuance of tokens is still unanswered by the EBA.

Mastercard's position is that SCA should not be required for issuing tokens or updating them as long as this process happens in the background without the payer's intervention. This is because:

- Such issuance/update of the token does not qualify as an action 'by the payer' within the meaning of Article 97(1)(c) PSD2. Article 97(1)(c) requires SCA "*where the payer* […] *carries out any action through a remote channel which may imply a risk of payment fraud or other abuses*" (underlining added).
- The updated token remains associated with the same user/device. Hence, there is no new association of security credentials with the user under Article 24(2)(b) RTS.
- The token replacement process is performed in a secure environment, which prevents fraudsters from intercepting and stealing the new token. Hence, such process does not qualify as an action 'which may imply a risk of payment fraud or other abuses' under Article 97(1)(c) PSD2.
- The payer expects that once her plastic card expires or is replaced with a new card with the same PAN and functionalities, she can continue shopping online without having to manually update all the tokens in her merchant card-on-file / wallet solutions.
- Requiring a new SCA for this process would have a very detrimental effect on the payment experience and cause disruptions for millions of consumers who rely on COF and wallet solutions to conveniently pay for products and services.

Mastercard's position is that registering a tokenized card on merchant's file or on a wallet solution, however, requires SCA under Article 97(1)(c) PSD2 (as the EBA confirmed in its Q&A 2021_6141).

Mastercard recommendation:

Regulators should answer / address the open question of SCA for issuance of tokens, and Mastercard is of the view that SCA should not be required for issuing tokens or updating them as long as this process happens in the background without the payer's intervention. This is because such issuance/update of the token would not qualify as an action 'by the payer' within the meaning of Article 97(1)(c) PSD2.

2.6. SCA delegation and outsourcing

The EBA clarified in its Opinion of June 2018 and through its Q&A tool that banks are allowed to delegate SCA to third parties. These include merchants (e.g., Amazon) and wallet providers / phone manufacturers (e.g., Apple - see EBA's Q&As 2020_5643, 2018_4047, 2019_4651 and 2019_4937). In particular, the EBA outlined that issuers may:

- "[U]*se third party technology, such as a smartphone fingerprint reader, to support SCA and to ensure they fulfill all the security measures established in the* [RTS]".
- "[O]*utsource the execution of SCA to a third party in compliance with the general requirements on outsourcing, including the requirements in the EBA Guidelines on Outsourcing*".

Mastercard's interpretation of these EBA's Q&As is that:

- If the issuer has its own app and authenticates the payer by relying on a third-party's technology (e.g., an RSA token generator or TouchID on an iPhone), this is not SCA delegation, nor outsourcing. In this case, the issuer is actually authenticating the payer and is only technically using the third party's authentication technology "*to support* [its own] *SCA*".
- If an issuer "*outsources the execution of SCA*" to a wallet provider (e.g., for Apple Pay) or a merchant (e.g., Amazon), this is SCA delegation. This is because, in this case, it is not the issuer that authenticates the cardholder, it is the wallet provider or the merchant. In principle, regulators could consider this SCA delegation as outsourcing under the EBA Guidelines on outsourcing. A contract between the issuer and the wallet provider/merchant would be needed and our Delegated Authentication program may be used to this end.

Mastercard understands that there is still uncertainty within the industry on whether SCA delegation qualifies as 'outsourcing' under PSD2. Our current approach is to leave PSPs to decide on a case-by-case basis whether SCA delegation to wallet providers or merchants is outsourcing. This is because PSPs are ultimately liable to comply with the regulatory requirements on outsourcing.

Mastercard believes that the regulatory framework should provide clarity on whether SCA delegation is outsourcing and clarify that, in any event, SCA delegation is not 'critical' outsourcing (which is subject to more stringent requirements under the EBA Guidelines on outsourcing).

Mastercard recommendation:

As there is still uncertainty within the industry on whether SCA delegation qualifies as 'outsourcing' under PSD2 the regulatory framework should provide clarity on whether SCA delegation is outsourcing and clarify that, in any event, SCA delegation is not 'critical' outsourcing subject to more stringent requirements under the EBA Guidelines.

2.7. GDPR and behavioral biometrics

Note: for additional and more detailed insights please review Appendix I.

Under the PSD2, it is clear that PSPs choosing to use behavioral biometrics as the second SCA factor (inherence, alongside a one-time password (OTP)) are in a strong position to comply with SCA requirements. However, a lack of clarification within PSD2 has created obstacles from a GDPR standpoint which prevents them from relying on such technology. In other words, legal

inconsistencies are hindering the development of sophisticated technological solutions meant to improve authentication methods.

- For additional information as to why the combination of behavioral biometrics and OTP is stronger than SCA solutions based on the knowledge and possession factor, we provide some description below:
    - Accuracy - This combination captures new types of fraud which would be hard to capture otherwise, for instance in relation to risks of social engineering
    - Security - It is considerably more secure as it is almost impossible to copy or replicate the data, similar to traditional biometrics (e.g. facial recognition, or fingerprint/iris scanning)
    - Inclusiveness - It is more inclusive and accessible especially as it does not require that devices be equipped with biometric sensors
    - Better payment experience - Ultimately, it helps reduce transaction failure/abandonment rates (and consequently reduces harm to consumers and merchants)
- These considerable benefits are only going to be able to materialize widely if the revised PSD2 addresses certain practical challenges stemming from the interaction of SCA with the GDPR.
- Specifically, Article 9 of the GDPR is understood to cover the processing of behavioral biometric data for SCA purposes which means that this data qualifies as a "special category of personal data", thus rendering it subject to a principled consent requirement.
- Such strict GDPR consent requirements create major practical challenges for deploying behavioral biometric data as part of SCA, including but not limited to the following:
    - Consent allows fraudsters to circumvent SCA based on behavioral biometric data processing as fraudsters may simply (and logically) not give their consent.
    - Consent requires the availability of alternative options that do not include the processing of behavioral biometric data. In practical terms, this means that PSPs must provide an alternative authentication method, which inevitably undermines the benefits of behavioral biometrics, and subsequently of SCA. Fraudsters and other malicious actors using sophisticated techniques could opt to use the non-biometric route and have a simple way of side-stepping the "knowledge" authentication method by exploiting password reset mechanisms.
- These steps are detrimental to consumers, the digital economy and the society at large, especially at a time where we are experiencing a growth in cyber threats and fraud attempts online.
- Against this background, Mastercard recommends that the PSD2 revision help secure a better legal ground for the processing of behavioral biometric data for SCA.
- More specifically, Article 9(2)(g) GDPR states:

  "…processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of

the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject ".

- Accordingly, the revised PSD2 Directive could include a clause explaining that payment security and SCA constitute a "substantial public interest" thus paving the way for a sustainable and robust alternative to consent, which is deeply flawed in this scenario.
- Concretely, we recommend the following wording is included in the new text:

  "For the purposes of preventing fraud the processing of special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725 shall be deemed a reason of substantial public interest according to Article 9(2)(g) of Regulation (EU) 2016/679, subject to appropriate safeguards for the fundamental rights and freedoms of persons, including technical limitations of the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation and encryption, where anonymisation may significantly affect the purpose pursued."
- By planting the seed for the legislative basis required for substantial public interest, the PSD2 revision would ultimately enable a better payment experience, one that is more secure, accurate, inclusive, and user-friendly.

Mastercard recommendation:

Mastercard recommends that the PSD2 revision help secure a better legal ground for the processing of behavioral biometric data for SCA.

***

Appendix I

Behavioural biometrics in Strong Customer Authentication – GDPR Challenges and Solutions

Summary

- Payment Service Providers (PSPs) who leverage behavioural biometrics as an inherence SCA factor alongside a one-time password (OTP) as a possession SCA factor are in a strong position to achieve effective, secure, frictionless SCA. However, a lack of clarification within PSD2 has created obstacles from a GDPR standpoint which restrict the use of such technology.
- Specifically, due to lack of clarity in PSD2, the processing of behavioural biometric data is currently interpreted as being subject to explicit consent under the GDPR. However, relying on individuals' consent may undermine the benefits of behavioural biometrics.
- Accordingly, Mastercard recommends that the PSD2 revision help secure an alternative lawful basis to consent for the processing of behavioural biometric data for SCA, and that the text of the revised PSD2 include a clause explaining that such activity may constitute a "substantial public interest".

Background

The Revised Payment Services Directive (PSD2) mandates strong customer authentication ("SCA") for remote payment transactions. SCA is authentication based on the use of two or more factors categorised as:

(a) knowledge: something only the user knows - e.g., passcode or PIN;

(b) possession: something only the user possesses - e.g., token, dynamic CVV, random code generated or sent to a previously registered device ("**OTP"**) or app/browser with possession evidenced by device binding; and

(c) inherence: something the user is - e.g., physical, physiologal or behavioural biometrics such as fingerprint, face, iris, eye vein or how a specific individual types, scrolls-down or holds their device.

Some SCA solutions capture behavioural biometric data (characteristics about an individual's interaction with their computer or smartphone device, including the use of their keyboard, mouse and/or the way in which they hold and interact with their device) as one of the two factors for authenticating individuals alongside a possession factor (e.g., an OTP). EBA regulatory technical standards have confirmed that **inherence may include behavioural biometrics** identifying the user.

Behavioural biometric data processing enables more effective, secure and frictionless SCA compared to knowledge-based factors (i.e., PIN or passwords). Specifically, the combination of behavioural biometrics (inherence) and OTP (possession) has the following advantages over SCA solutions combining the knowledge and possession factors:

- **Accuracy -** This combination captures new types of fraud which would be hard to capture otherwise. This includes **reduced risk of social engineering/fraud** and **reduced transaction failure/abandonment rates.**
- **Security** - It is considerably more secure as it is almost impossible to copy or replicate the data, similar to traditional biometrics (e.g., facial recognition, or fingerprint/iris scanning).
- **Inclusiveness**- It is more inclusive and accessible for all individuals than other forms of inherence used for SCA, especially as it does not require that devices be equipped with biometric sensors.
- **Better payment experience** – It improves consumer experience by reducing transaction failure/abandonment rates.

These considerable benefits may only materialize widely if the revised PSD2 addresses certain practical challenges stemming from the interaction of SCA with the GDPR and associated with the processing of behavioural biometrics.

Behavioural Biometric Data under the GDPR

Any biometric data collected or processed for the purpose of uniquely identifying a natural person, in connection with SCA is likely to constitute a special category of personal data under the GDPR. "Biometric data" is defined in Article 4(14) of the GDPR and includes "behavioural characteristics."

There are additional requirements for special category personal data under the GDPR. PSPs need to establish a lawful basis for processing under both Articles 6 and 9 when processing behavioural biometric data for the purposes of authenticating individuals' identities.

In the context of processing behavioural biometric data for SCA purposes, the only lawful bases of processing from Article 9 that could be relevant are:

- Article 9(2)(a) – data subject's explicit consent to the processing; and
- Article 9(2)(g) – processing is necessary for reasons of substantial public interest.

Option (a) – Consent

For the purposes of the GDPR must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes". "Freely-given" means that the data subject must have a genuine choice as to whether their personal data is processed in a certain way.

Using consent as a lawful basis for the provision of a service does not meet the requirement for consent being "freely-given". Moreover, withdrawal of consent should not lead to a data subject being penalised or suffering detriment. European Data Protection Board (EDPB) guidelines on consent state that the availability of alternative services provided by third parties that do not require consent for processing is not sufficient freedom of choice to render consent freely given. Consequently, relying upon consent for processing behavioural biometric data would necessarily require the availability of alternative authentication options that do not comprise the processing of behavioural biometric data. For the purposes of SCA, this means a PSP would have to provide an alternative authentication method to behavioural biometrics, likely based on the "knowledge" authentication factor.

Providing an alternative method of authentication in the customer journey would significantly diminish the benefits of behavioural biometrics. It has been proven that reliance on knowledge based SCA reduces transaction acceptance rates and increases the risk of transaction fraud. Fraudsters

would likely use the non-biometric route and have a simple way of side-stepping the knowledge authentication method by exploiting password re-set mechanisms.

These steps are detrimental to consumers, the digital economy and the society at large, especially at a time where we are experiencing a growth in cyber threats and fraud attempts online.

Option (b) – substantial public interest

The other available lawful basis for processing behavioural biometric data is a "substantial public interest". A substantial public interest is identified where an activity benefits the society at large. There are strong grounds to argue that behavioural biometrics benefit society, as the more secure the remote payment transactions, the more benefits for the consumers, the merchants and the entire payment ecosystem.

To meet the requirements of this lawful basis under the GDPR, the processing of behavioural biometric data must be **necessary** for the substantial public interest **on the basis of union or member state law**. In other words, to rely on substantial public interest, there needs to be a legislative provision in a legal instrument outside the GDPR that clarifies why there is substantial public interest in processing that type of data.

Accordingly, we recommend that the revised PSD2 Directive include a clause explaining that for remote payment transactions, the processing of special categories of data for fraud prevention and SCA purposes constitutes a "substantial public interest". Such clause will pave the way for a sustainable and robust alternative to consent. Concretely, we recommend the following wording is included in the revised PSD2:

Recommended Wording: "For the purposes of Strong Customer Authentication and fraud prevention, the processing of special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725 shall be deemed a reason of substantial public interest according to Article 9(2)(g) of Regulation (EU) 2016/679, subject to appropriate safeguards for the fundamental rights and freedoms of persons, including technical limitations of the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation and encryption, where anonymisation may significantly affect the purpose pursued."

By planting the seed for the legislative basis required for substantial public interest, the PSD2 revision will ultimately enable a better payment experience, one that is more secure, accurate, inclusive, and user-friendly.

***