MRC Response to RBA Issues Paper Consultation of June 2023 on Default Settings & Tokenisation

About the MRC

MRC is the go-to place for eCommerce payments and fraud professionals across the globe. We are a global nonprofit membership association for payments and fraud prevention professionals. The company was established in 2000 with several US retailers coming together to discuss fraud trends and share data. We now have nearly 700 members in the U.S., Europe, APAC, LATAM, and beyond, including 85% of the top eCommerce global brands. The members include retailers, card issuers, acquirers, payment service providers, fraud solution providers, law enforcement agencies, regulators, and payments consultants.

The strength of MRC membership lies in staying connected, current, and empowered to influence and transform the industry. To that end, the MRC places great importance on its core pillars:

Collaboration: Building a spirit of trust and collaboration. Facilitating open conversations about industry issues and information sharing among members are critical when it comes to influencing the future of eCommerce.

Networking: We strive to continuously offer proven and innovative ways to connect with and learn from industry stakeholders worldwide. Our members can expand their network at our in-person and virtual events through a discussion forum and community groups, speed-networking events, etc.

Education: One of the goals of the MRC is to serve as an educational resource for payments and fraud prevention professionals of all levels. Our programs like the accredited RAPID Edu eLearning courses help make that possible.

Advocacy: With the ever-evolving nature of the payments industry, new regulations, standards, and policies continue to change and become more complex. Advocating for our members is of utmost importance to us and has proven to benefit the payments industry across the board.

MRC response to RBA Issues Paper

MRC acknowledges the importance of the work carried out by the RBA for the payments industry, particularly with efforts to make the ecosystem more secure and safe for both merchants and consumers. The MRC, and our members, are excited about the promise of better security for consumers and fewer fraudulent transactions.

We agree with the RBA that a solution is needed, and we wish to work with the RBA, in conjunction with our merchant members, to identify what that solution is. We further agree that tokenisation is an excellent security measure and to ensure its successful implementation into the ecosystem, all related issues and concerns, from all stakeholders, should be identified and resolved, within a reasonable time.

Customer data must be kept secure. We are aware of at least three high profile data breaches in Australia recently, which has heightened the need and want for new security measures. MRC continues to encourage merchants to use all security tools available to them to ensure payment fraud is effectively detected and prevented. Payment Card Industry Data Security Standards (PCI DSS) were introduced to resolve this very issue. Ensuring compliance with these standards, and the correct storage of PAN is key to avoiding such data breaches.

MRC Merchant Member Concerns

On July 18th, MRC held a meeting with 10 merchants including global brands operating in Australia, and local brands to the region. The purpose of the meeting was to get the merchant viewpoint on the expected impact of a blanket tokenisation solution for general card payments.
Concerns were raised, in particular in relation to the consumer impact, and to the ability for merchants to manage disputes and refunds after transaction data has been tokenized; among other things.
We bring the concerns and questions raised to your attention here.

Eftpos – Regarding dual network debit card routing, if eftpos does not have a tokenization solution available by the end of 2024, what does that mean for merchants if a mandate is enforced by that time? Will the RBA consider a new date? Will merchants be required to push DNDC transactions to the more expensive network options?

Who can hold the data? – The issues paper refers to the RBA not being comfortable with merchants storing card credentials. Is it the case that there is comfort with acquirers storing the data?

When can merchants hold the data? - The RBA issues paper appears to be pro-network tokens over merchant tokens. If a merchant builds their own data vault for tokens, would they be able to retain the data, or would they still have to outsource to a third-party supplier under a potential mandate?

On timing – compared to tokenization implementation in India, merchants attending the meeting noted they also process in India and the experience thus far with the implementation of tokenisation on card payments there, is a negative customer experience. Merchants work around legislation while endeavouring to implement change within an impossible time limit. The concern here is the RBA timelines for 2024 are equally tight. The ecosystem does not have the time needed to build, test, collaborate across industry, to effectively deliver a consumer-friendly card payment environment.

Merchants are fine with tokenisation, but requiring its implementation at speed may mean workarounds are required by merchants. Having choice is important for merchants.

Other effective security measures – If card data is stored in a PCI environment, there should not be a requirement for tokenisation as well.

Motivation? – It was raised, why should merchants move to a token-only world? What is the motivation for the proposed mandate? Identifying the problem, will help the industry produce the right solutions, with multiple security measures, fit for purpose.
It was raised, there are other ways in which customer data is captured, which tokenisation does not fix, e.g., social engineering fraud.

There is a consensus that merchants are in favour of tokenisation being a merchant choice, not a mandate.

Consumer Impact – Case Studies

Customer experience – Practice shows performance and success rates using tokenisation are not near, or equal, to transactions on PANs. This is true for both one-off and reoccurring transactions.

The real impact elsewhere – A distinction was noted between what the RBA and AusPayNet have requested versus what the RBI requires in the recent India example. For cross-border transactions, the Reserve Bank of India (RBI) views all transactions the same. The frontline experience is the moment regulation is applied to cross-border transactions there is disruption and a higher rejection rate.

Identifying the transaction later – Merchants raised that in some cases the consumer transaction relates to a product or service to be delivered to them well into the future, e.g., airline ticket, concert pass, or to a transaction that may require a future action such as posting winnings after a bet.
In a case example provided, if a customer raises an issue with a transaction that took place 6 or 12 months ago, the merchant needs to be able to relate their query back to the original transaction. If a refund is required, they must be able to apply the refund to the original source. Removing the PAN from merchant records is shown to impact the consumer experience in this regard.

Merchants need to retain card data for safe and valid processing of refunds and dispute resolution.

Transaction retries and consumer friction – merchants want the consumer experience to be seamless. In the event a token-based card transaction fails, the merchant cannot retry the purchase. Holding the PAN record on file allows the merchant to use standard retry methods, to ensure service to the consumer is uninterrupted. Without the PAN, a merchant can't identify the reason for a failed transaction or help the consumer to resolve the issue at their end. The consumer experience results in a negative one.

Retaining PAN for fraud prevention – it is practice for merchants to use stored PAN details to help identify fraud, using machine learning and data engineering. The PAN can help merchants identify if particular card issuers are being targeted and in practice they engage and collaborate with issuers to help mitigate against such attacks.

Conclusion

MRC very much welcomes this opportunity to engage with the RBA on this important topic and remain at your disposal for any further discussion on the matter.

We would appreciate a further opportunity to facilitate open discussion with merchants in Australia, with whom we work, to ensure they have had the appropriate time to consider all the potential impacts of a potential mandate on tokenisation, and to help communicate to you their specific concerns and issues, as well as their frontline real case examples where the consumer is negatively impacted when tokenisation is used as a blanket solution, rather than part of a multi-faceted group of solutions.

We are scheduled to have a call tomorrow, August 27th, with representatives from the RBA, and with our merchant members to talk about the questions the merchants have raised with us. We are very grateful for this openness and collaboration with the RBA.

MRC will continue to provide you with the merchant, and wider industry, perspective and to facilitate future meetings to ensure the industry collective voice is heard and delivered.

We thank you sincerely in advance of your consideration to further look at tokenisation as a fix-all for card payment security, and our member concerns and questions.

Contact:

Úna Dillon|VP Global Expansion & Advocacy, MRC.
Advisor to European Commission PSMEG
MRC | www.merchantriskcouncil.org| Ireland
Email: una@merchantriskcouncil.org |Tel: +353.87.204.7579
MRC: Where Payments and Fraud Prevention Professionals Come Together