MasterCard Europe's contribution to the European Central Bank consultation on the "Recommendations for the security of internet payments", in the context of the work undertaken by the European Forum on the Security of Retail Payments.

Introduction

MasterCard Europe provides the technology, expertise and flexibility for cardholders, merchants and their banks to transact business anytime, anywhere, including online. As franchisor, processor and advisor, we deliver solutions for consumers and businesses who seek faster, more secure and smarter payment methods for the widest possible range of goods and services.

We would like to thank the European Central Bank (ECB) for offering to us this opportunity to contribute to the policy dialogue relating to the security of internet payments. In bringing safe and efficient pan-European payment solutions to millions of European consumers and merchants, MasterCard Europe is fully engaged in and committed to facilitating the establishment of a secure electronic retail payments market.

We welcomed the establishment in early 2011 of the European Forum on the Security of Retail Payments at the suggestion of the ECB. We believe that this voluntary cooperative initiative between relevant European authorities has played a constructive role in facilitating common knowledge and understanding of issues related to the security of electronic retail payment services and instruments. Regarding a number of the recommendations raised in the report on the security of internet payments, we are pleased to be able to inform the ECB of developments and progress that MasterCard Europe, individually and in concert with other industry actors, is introducing in order to contribute to fighting payment fraud and enhancing consumer trust in such services.

General Comments

It is clear that considerable work has been put into the detail of this ECB report which has many points in favour of adoption. There are, however, a few points we would like to raise both in clarification and perhaps taking a slightly different stance which we believe would benefit production of a final version.

Evidently, the intention of this report is to develop an environment of strong authentication across internet payments in Europe. Past experience has shown that there considerable work is needed to achieve this and to ensure that any new framework does not form a barrier to sales during deployment, whilst also focussing on the main intent of combating fraud.

We believe that the proposed date of 1 July 2014 for implementation by PSPs and card payment schemes of the recommendations within this report may be very challenging even if formal publication of the requirements were to occur in the near future.

Payment Service Providers (PSPs)

MasterCard Europe understands that the ECB may wish to keep the definition of what constitutes a payment service provider (PSP) to the broadest stance ensuring all stakeholders are captured. However, we believe that the full context and content of the recommendations would not be able to be fulfilled by all that are captured by this definition. For example, the authentication of the account

or card holder would have to be the responsibility of the institution that has the primary legal relationship rather than other parties such as a merchant or acquirer.

If the intent of the report is that any party to the payment process should fulfil any responsibility under which it would be reasonable for a regulator to expect them to have control then this report makes sense. However, it may be worth clarifying this point as there are parties within the payment industry known as Payment Service Providers, or PSPs, that act on behalf of a merchant to facilitate the payment. These entities can certainly facilitate authentication of the account holder by deploying the correct industry solution, such as *3D-Secure*, but could not undertake the actual authentication themselves, nor could they impose a practice onto the merchants or issuers. Therefore, recommendation 7.5K cannot be imposed. Also to note that the mandated use of CVx2 is not feasible given that not all cards carry CVx2, and given that – in the context of a wallet - this code cannot be stored by the wallet provider.

Risk Based Authentication (RBA)

We are pleased that the concept of authentication based on risk is within the recommendations of the ECB. Within this report, the ECB has taken a stance that RBA should be used to determine the strength of authentication that should be used or allowed. We support this view as one option of RBA, but strongly believe that a fundamental issue has been overlooked.

MasterCard Europe believes that the purpose of authentication is to prevent fraud and have a number of solutions that support authentication of a cardholder using both static and dynamic authentication. We have also take a position on RBA and published a paper on this that discusses the fundamentals of authentication and suggesting that it is acceptable for an Issuer or Merchant to not require authentication on a transaction that they deem to be low risk, as long as they are willing to accept the liability on any transaction where they are in error without question.

Under MasterCard Europe's existing rules for RBA, an Issuer has the opportunity to authenticate their cardholder using non-static data or decide to move forward without interaction with the cardholder. The Issuer in this circumstance would be authenticating the transaction on behalf of their cardholder and this would result in a Fully Authenticated transaction for the merchant with liability resting with the Issuer.

MasterCard Europe has also developed a programme for merchants, known as *MasterCard & Maestro Advanced Registration Programme* or *MARP*. This program actually recognizes that some merchants have already implemented very efficient risk and fraud management solutions, and allows these merchants to implement a more flexible authentication strategy while at the same time enhances the customer experience. Once accepted to the programme, the merchant is required to obtain authentication for the first transaction undertaken with any customer. After that the merchant have the option to undertake standard authentication or, if they deem the transaction as low risk, proceed without further authentication. This is specifically flagged within MasterCard's authorisation system as liability will rest with the merchant.

This ensures that MasterCard would be able to monitor the environment to ensure that fraud was kept to a minimum removing this option from any participant that was not able to fulfil defined conditions. Our RBA approach requires the use of dynamic authentication for those transactions that are authenticated and MasterCard is already investigating ways by which to provide Enterprise-based solutions to help stakeholders deploy successful solutions.

We believe that this should be an option for any party that fulfils defined criteria and that the ECB should adopt this approach widening the use of RBA not just to the strength of authentication but to when authentication should be undertaken.

Preventing Fraud by Monitoring Transactions

MasterCard fully supports the Third Guiding Principle and Recommendation 10 for the implementation of effective processes for monitoring transactions in order to identify abnormal customer payment patterns and prevent, detect and block fraudulent payment transactions in real time. However, MasterCard wishes to draw the ECB's attention to Article 20 ("Measures based on profiling") of the European Commission's proposed General Data Protection Regulation, which could potentially hamper the implementation of the processes recommended under the report. This proposed provision uses overly vague criteria and, as a result, will have an overreaching scope of application, as it will capture the majority of antifraud tools. Those tools are indeed based solely on automated processing (real time monitoring) of personal (transactional) data intended to evaluate an individual's payment pattern (i.e. his or her "behaviour" as meant under the proposed Regulation) and may be deemed to produce "legal effects" or that "significantly affect" said individual (e.g. the denial of the transaction). Where no direct contractual relationship exists between the payment system/service provider and the individual (which is the case for MasterCard, for example), the express consent from that individual – including that of the fraudster – would need to be secured for the use of antifraud tools, except where Member States' national law *expressly* permit the processing of personal data when this is necessary to safeguard the prevention, investigation and detection of payment fraud, in furtherance of Article 79 of the Payment Services Directive.

Neither the express consent of the individual nor an express authorization under a Member State's national law provide for the adequate and flexible regime that payment systems and payment service providers need to deploy and apply antifraud tools which are essential to ensure the security and reliability of their service, and which, in turn, are essential to build and strengthen consumers' trust in the digital economy.

The ECB should thus call for the "profiling" regime under the proposed General Data Protection Regulation to be realigned on the general regime, i.e. to allow the data controller to rely on its legitimate interests as a valid legal basis for processing personal data. Those legitimate interests should further be expressly stated to include the monitoring and prevention of fraud. Such clarifications would ensure that Recommendation 10 can adequately and effectively be implemented by payment systems and service providers.

Further potential programme developments from MasterCard

MasterCard Europe is currently exploring options that could add further expansion to its *MasterCard SecureCode programme* that would ensure that any transaction that was attempted by a merchant had explicit evidence for the Issuer. By doing so, it should be possible to ensure that the programme was followed by providing a token to the merchant (known as an *AAV*) for all attempted transactions as well as the current process for Fully Authenticated. This would then be included in any authorisation message submitted by the merchant. This could be a good technical enhancement that would ensure the integrity of the authentication and subsequently, the payment environment. Further expansion may also include a history of every authentication attempted and the result of that attempt that would be available to the Issuer in case of dispute.

Concluding remarks

MasterCard Europe believes that a balance of technology, information and rules will move electronic commerce transactions to an environment where each transaction will be unique protecting all participants in the transaction. We also share the belief that these solutions need to be capable of rapid evolution given the growth in new channels, such as mobile payments, that we believe will grow rapidly in the near future.

The payments industry has invested significant amounts over the years in the development of security features for electronic commerce. MasterCard Europe believes that, as a result, these types of transactions are sufficiently secure. However, fraudsters are working hard to constantly try to outwit the security measures that are put in place. Therefore, market players are forced to continue to invest in security features, and this process will never end, i.e. the payments industry will always need to be investing in order to enhance security features.

In the case of electronic payments, there needs to be a careful balance between security measures and consumer "ease of use". This balance is best placed in the hands of the schemes and Issuers, which are in a position to judge when too much security impacts consumer experience and consumer use of electronic payments.

MasterCard Europe would like to again thank the ECB for this opportunity to contribute to the policy dialogue, and we would be delighted to continue to play a constructive role in developing strong authentication for the security of internet payments in Europe.

MasterCard International

Chaussee de Tervuren 198A
1410 Waterloo, Belgium

Mikael Conny Svensson
Senior Business Leader Government Affairs and Public Policy
E-mail: mikael_svensson@mastercard.com