E-COMMERCE TRANSACTIONS – A NEW ROADMAP FOR AUTHENTICATION IN EUROPE

Christoph Baert, Paul Baker and Cathy Mulrow-Peattie co-authored this article.

New regulatory measures requiring strong authentication for e-commerce transactions will make authentication a key focus for issuing and acquiring banks, merchants and consumers in Europe. The aim of this regulation is to reduce fraud in online payments with strong authentication, or, alternatively, a risk-based approach to authentication as long as this is effective in controlling fraud. The focus for MasterCard and its customers is on providing safe, simple and consistent consumer experiences that balance these needs.

MasterCard SecureCode, MasterCard’s online authentication solution, is based on the cross scheme 3D-Secure standard and already fulfills the new requirements. MasterCard has a suite of products that can support customers’ needs to undertake strong authentication. As MasterCard develops and releases new products into the European market, the goal will be to ensure that those products are compliant with the new regulatory framework and with a roadmap for any further regulatory changes.

The new European measures on authentication are contained in the draft Revised Payment Services Directive (PSD2) and in the European Banking Authority’s Guidelines on the security of internet payments (EBA Guidelines).

The PSD2 and the EBA Guidelines contain similar authentication requirements. The EBA Guidelines were issued in December 2014 and will apply to customers in most EU countries on Aug. 1, 2015. We are waiting for the issuance of the final version of the PSD2, which will apply to customers in 2018, with an exact date of compliance yet to be issued.

What is MasterCard’s authentication strategy and how is it impacted by the current regulatory changes?

MasterCard’s existing global authentication strategy consists of a risk-based approach. If authentication is necessary to prevent fraud on a transaction, and where the risk indicates that authentication should occur, we believe that overtime this all should be based on non-static authentication. The approach taken by the European regulators is similar to MasterCard’s global strategy, and we believe that this is an opportunity to resolve issues that have been challenging the e-commerce space. More specifically, those issues include the fact that passwords are difficult to remember and are easily stolen and/or hacked.

MasterCard believes that authentication is effective and necessary if used in an appropriate way. MasterCard has been developing various options -- like biometrics -- that provide both an effective and an easy to use solution. It is clear that authentication can change approval rates from the low, circa 80 percent, seen today for remote payments to those of face-to-face or higher, circa 96 (MasterCard Data 2014). The risk-based approach allows MasterCard and its customers to balance this against the risk of consumer online shopping cart abandonment if authentication is overused and becomes too difficult to use.

MasterCard is pleased that it already supports both the risk based approach and strong authentication today.
What is defined as strong customer authentication?

The PSD2 and the EBA Guidelines define strong authentication as authentication through at least two out of the following three factors:

- Something only the user knows like passcode or PIN;
- Something only the user possesses; like mobile phone or token; or
- Something the user is; like a fingerprint.

The PSD2 and the EBA Guidelines require that the selected factors must be mutually independent in that the breach of one does not compromise the reliability of the other.

Although the legal definition of strong authentication is largely the same, there are two differences between the PSD2 and the EBA Guidelines in relation to the authentication factors.

1. First, the EBA Guidelines dictate that at least one of the factors used should be:

   “Non-reusable”;
   “Non-replicable (except for inherence)”;
   “Not capable of being surreptitiously stolen via the internet”.

   These conditions, which are not required under the PSD2, are difficult to meet in a world where information lives on the internet and can easily be replicated like in an e-commerce transactions.

2. Second, the PSD2 sets forth an even more stringent requirement: strong customer authentication for electronic remote payment transactions must include elements linking the authentication to a specific amount and a specific merchant in the form of a dynamic code.

When will strong authentication apply?

Under the EBA Guidelines, strong authentication will apply to the initiation of internet and mobile browser-based payments, virtual card payments, the registration of card payment data for use in digital wallets, and access to sensitive payment data.

Under the PSD2, strong authentication will apply to access to payment accounts online, to the initiation of any electronic payment transaction, and to any action through a remote channel which may imply a risk of payment fraud or other abuses, including online or mobile payments.

Which transactions will escape strong authentication?

While strong authentication will be the rule for e-commerce transactions, the use of alternative authentication measures will be permitted only as a way of exception. The PSD2 and the EBA Guidelines allow customers to use alternative authentication measures for specific categories of transactions.
In particular, the EBA Guidelines allows alternative authentication measures for low-risk or low-value payments. The PSD2 allows alternative authentication measures also on the basis of the recurrence of the transaction and the payment channel used for the execution of the transaction.

The EBA will be responsible for identifying and setting out guidelines regarding the transactions for which alternative authentication measures are allowed.

**How strong is strong authentication?**

Devices generating one-time passwords (OTPs) or and biometrics are commonly considered to be more secure than static passwords.

For example, OTPs do not directly authenticate consumers; they are machine-generated by a token device or a mobile phone. What really authenticates consumers is the procedure that gives them access to the device or system that generates and/or communicates the OTP. This is why some OTP systems are stronger than others. An OTP that is sent to the user via e-mail is only as strong as the authentication that protects anyone from getting access to that e-mail (usually, only a static password).

The same reasoning is true for biometrics. Like with OTPs, it is illusory to think that the best level of security can be achieved by replacing static passwords with any biometric. With biometrics, security depends on the strength of the biometric, on the device or method through which the user authenticates, and its resistance to being tampered.

It is also clear that there are a number of devices that include a Cardholder Verification Method or CVM to open the phone and that this could be an opportunity for these to be used by the consumer to authenticate themselves for a payment. MasterCard has been working on setting network security standards of a shared CVM which examine both the types of CVM in use (Biometric, Swipe pattern or PIN) and the technical requirements for the devices to create a standard that could allow these to be used as authentication by an issuer for a payment, in a similar way to that shown within the Apple Pay environment.

**What's the impact on convenience and user experience?**

The user experience may be significantly affected by the authentication process that the consumer must go through during an online transaction. Security must be balanced with consumer convenience during the online transaction authentication process. For example, authentication solutions that involve special hardware devices such as cap readers or tokens may be appropriate when consumers are transacting from their PCs at home, but may be much less appropriate for transacting with mobile devices “on the go” or in-store.

**An alternative risk-based assessment**

Authentication should be seamless. Today, MasterCard customers can determine if a transaction is legitimate on the basis of objective criteria including purchasing patterns, fraud history and device parameters using legitimate data sources. Why would either a merchant or a bank wish to challenge a consumer transaction that has occurred many times before, where no fraud has occurred, all device parameters are the same, and the transaction amount is in line with normal purchasing’s patterns on that card?
The optimal solution would be to adopt a risk-based assessment where a transaction is subject to or excluded from strong authentication on the basis of a set of criteria set by the customer and where customers are incentivized to proactively monitor fraud levels to determine which authentication measures are required in relation to each transaction.

Such approach has proven to be efficient in several countries where a large number of security layers are already in place and allow customers to accurately determine the risk for each transaction. Many of these risk-based security layers provide a high level of protection against fraud while remaining invisible to a great majority of legitimate users. By analyzing a range of data in the context of each transaction, MasterCard customers may identify the likelihood of potentially fraudulent activity on a transaction-by-transaction basis. If the transaction is found to present a low risk of fraud pursuant to the authentication policies established by the customer, the transaction is allowed to continue unchallenged. Under this proposed solution, only potentially risky transactions would require strong authentication. We hope to work with the EBA on ensuring that this proposed solution would be part of its further guidance on PSD2.

**Conclusion**

Security is an important challenge for the electronic payment industry and represents one of the main battlefields for gaining the consumers’ trust in electronic payments. The user experience is strongly affected by the trust and confidence the consumer feels when making a digital purchase with a payment card. However, consumer’s safety should be balanced with convenience.

Strong authentication for every single card transaction is not necessary – be it for consumers (who favor payment solutions that are convenient and secure), merchants (who bear the risk of consumers dropping off and not making a purchase), customers or card schemes. Best results can be achieved through continuing to invest in a risk-based assessment as part of the strong authentication process and managing the consumer experience. MasterCard is working across payment networks with the global standardization body EMVCo to ensure that digital payments and their related authentication is a great experience for consumers. MasterCard is also working with its customers to offer risk based fraud assessment tools to help manage through these new regulatory measures.

A set of questions and answers is included at the end of this article that covers our existing products and may answer further questions on these new regulatory measures.