Recommendations for improving European online payments regulation

A collaborative effort by the following associations:

ECOMMERCE EUROPE

EDiMA

EPIF
European Payment Institutions Federation aisbl

Choice in eCommerce
Initiative for Choice and Innovation in Online-Trade

CCIA
Computer & Communications Industry Association
Tech Advocacy Since 1972

Commissioned to and prepared by:

CleverAdvice

Executive Summary

According to available data, the payments industry has effectively managed online risk, with payment fraud rates consistently declining at the European level over the last 6 years. Regardless, the European Banking Authority has mandated strict guidelines that require Strong Customer Authentication (SCA) for a number of online payment transactions.

SCA is a strict and burdensome process, requiring customers to actively intervene in authenticating all transactions regardless of their risk. This negatively impacts the customer's online experience and results in increased transaction abandonment.

A valid alternative to SCA is Targeted Authentication, which applies authentication techniques commensurate to the risks associated with each transaction, adjusting the level of customer intervention accordingly. Targeted Authentication has proven to offer fraud prevention levels matching those of traditional strong authentication techniques without deteriorating customer experience, ultimately leading to higher conversion at checkout.

Regulators can ensure a high level of security and a low level of fraud by setting a quantitative fraud rate level. Payment service providers that achieve levels of payment fraud at or below the determined rate should be allowed to offer authentication techniques alternative to SCA.

This would provide more tangible benefits for consumers now and in the future than mandating a technique and foster ongoing development of innovative fraud prevention solutions against continuous and increasingly sophisticated fraudsters' attacks.

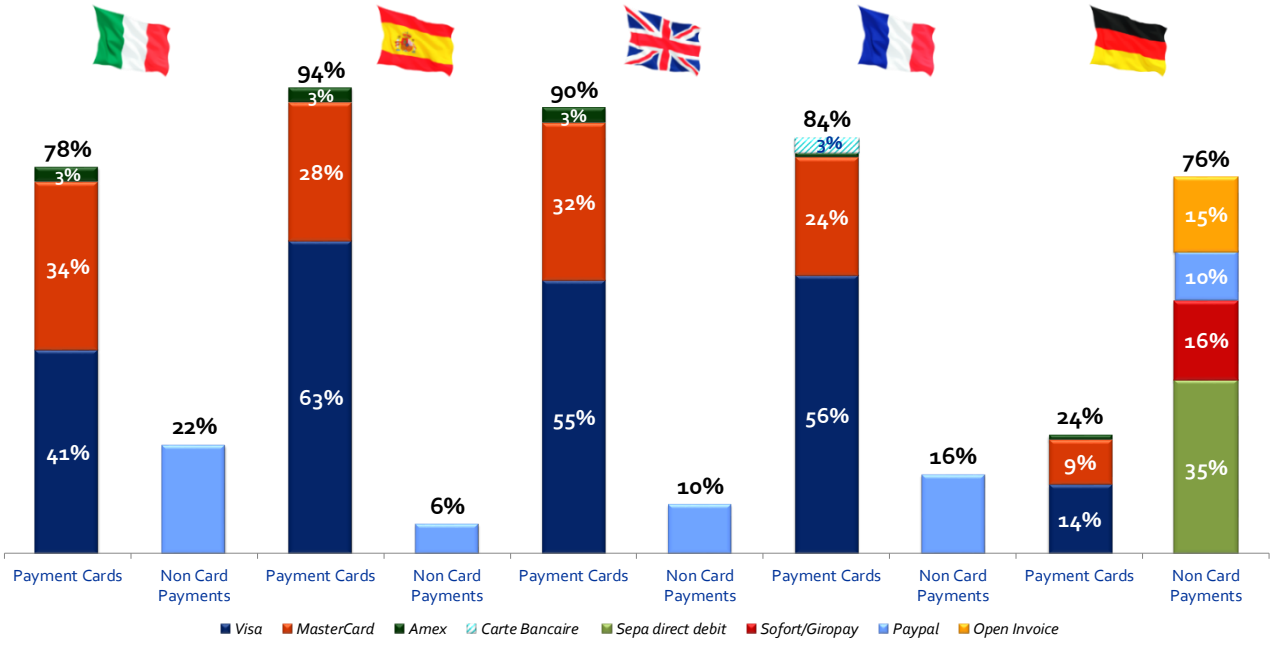
The opportunity to offer authentication techniques that bring higher conversion would also stimulate investments in innovation, healthy competition and e-commerce growth in Europe.

Introduction

An assessment of online payments fraud is key to understanding whether further actions are needed to increase the security of online payments and their urgency.

Except in Germany, the majority of Europeans pay for online purchases using their payment cards. In Germany, approximately 2/3 of online payments are settled using direct debits, payment initiatiation service providers and payments on delivery *(Fig. 1)*. In addition, a significant amount of PayPal transactions are backed by card payments, which makes the actual share of online payments value attributable to payment cards higher than shown in Fig. 1.

Figure 1: Online payment methods in the EU-5 countries

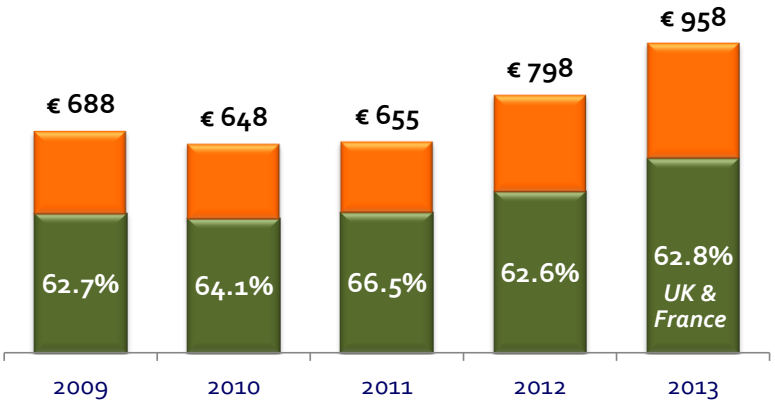


Source: Adyen, global-ecommerce-payments-guide-2015

Given that payment cards are very widely used to pay for internet purchases across Europe, any results or problems related to online card fraud can be extrapolated to online payments fraud.

In July 2015, the European Central Bank (ECB) published its fourth report on card fraud, which highlights that in 2013 the total value of fraud of Card Not Present (CNP) transactions related to cards issued within SEPA stood at € 958m, a 39% increase from 2009 *(Fig. 2)*.

Figure 2: Card Not Present Fraud for payment cards issued within SEPA (€m)



Source: ECB 2015

Growth in overall CNP fraud value is the main reason behind the ECB's stringent SecuRe Pay recommendations (made mandatory through the European Banking Authority's (EBA) guidelines aimed

at increasing the security of internet payments), which mandate Strong Customer Authentication (EBA, 2014, p. 11) for a number of transactions and events as of 1 August 2015. The EBA has stated that delaying the requirements until the transposition of the PSD-2, a suggestion brought by several national payment associations and leading industry players, would not be considered in light of the perceived risk to be addressed.

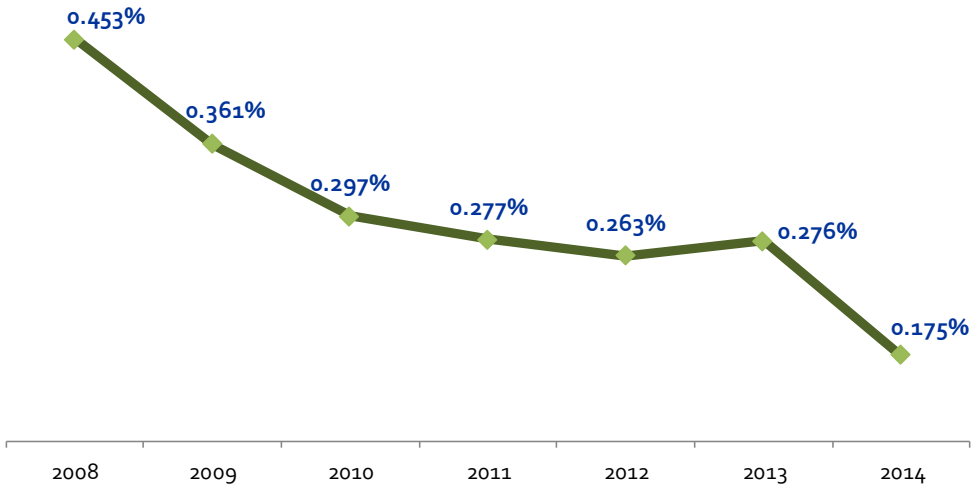
We believe that because these guidelines have a strong impact on both online payments and the e-commerce industry, they should be based on significant hard data. These should include CNP, and in particular internet payment fraud rates (not just values) at the European level since the EBA guidelines specifically address internet payments. Both figures are only partially available: CNP transaction values are available only for some countries, and not all national card schemes split CNP fraud into internet and mail or telephone fraud[1]. As a result, it is not possible to assess whether fraud rates for CNP or internet payments have increased or declined at the European level and as such there are no figures to back Europe-wide decisions. Furthermore, there is no clear indication available nationally or from industry as to whether a fraud increase is purely organic or caused by new threats

Use cases of France and the UK

A deeper understanding of internet payment fraud at the EU level is paramount to supporting any regulatory intervention. This may be achieved by taking a deeper look at countries that both report a split of CNP fraud showing internet payment fraud data and generate a large amount of online card payments value. France and the UK are good use cases: both publish official detailed card fraud data and account for 50% of the EU-28 e-commerce payment value (Ecommerce Europe, 2015), over 88% of which is paid using payment cards, 84% in France and 90% in the UK (Adyen, 2015). In addition, France and the UK combined generate nearly 63% of the CNP fraud value within SEPA (Fourth report on card fraud ECB, 2015).

Taken together, online card payments value generated by cards issued in France and the UK combined has grown on average at 31.2% per year over 2009-14 (+290% over the 5-year period), while card value lost to fraud experienced a more limited 13.6% yearly average growth rate (+89% over the 5-year period). Therefore fraud rates for online transaction value of cards issued in France and the UK combined have declined at an average rate of 13.5% per year, an overall decline of 51% *(Fig. 3)*. Online fraud rates at single country level confirm the downward trend.

Figure 3: Fraud rates of online transactions value generated by payment cards issued in France and UK



Source: UK Card Association, Observatoire de la sécurité des cartes de paiement

[1] The Fourth EBC report on card fraud states "*... based on this partial information, ...*" (p. 2) and "*... taking into account data for only those schemes reporting a split of CNP fraud into internet and mail or phone fraud, ...*" (p. 12)

European data suggest that cyber criminals target countries with high card usage, as reported in the latest ECB card fraud report: *"Most of the countries with mature card markets (defined as countries with high volumes and values of card transactions per inhabitant) experienced high rates of fraud"*. Both France and the UK generate very high payment card transaction values, so it is not surprising that they show the highest card fraud rates within SEPA (6.9 bps for France, 6.3 bps for the UK). According to ECB data, other countries – which are experiencing lower overall fraud rates – are likely to show similar or better trends regarding online card fraud. Therefore, when other countries' data are added to those of France and the UK we would expect to result in lower – or at least not higher – EU-wide internet fraud rates.

These analyses suggest that the payment industry is handling online risk effectively and that it has been able to reduce the impact of fraud by constantly lowering the online fraud rate in an e-commerce environment that has experienced exceptionally high growth in both values and volumes in recent history. As such, the analyses do not suggest the need for urgent regulatory interventions at the EU level.

As discussed in the paragraphs below, strict regulatory mandates such as those included in the EBA guidelines will potentially slow adoption and usage of online payments and the development of e-commerce. This is due to required customer intervention in the authentication process, which may involve multiple devices interfering with the shopping experience and making it more difficult to finalize the purchase. In addition, this is likely to limit innovation and prevent healthy competition within the industry and to potentially create barriers to a robust development of the digital economy in the EU, one of the main objectives of the European Commission.

We claim that SCA should always be an available option to ensure customer choice, but Payment Service Providers (PSPs) should also be allowed to offer alternative authentication and verification techniques where adequate customer guidance is provided. We recommend that alternative fraud prevention mechanisms should be considered viable to stimulate the development of customer authentication and verification processes, which offer high levels of security in the context where they are applied while retaining a satisfactory customer experience. This is critical to promote the e-commerce industry growth and set the basis for an ecosystem that stimulates the development of the digital economy in the EU.

In addition, we strongly recommend implementing standard fraud metrics and prevention guidelines to allow PSPs to conduct self-assessments of the effectiveness of the authentication techniques they have deployed, based on quantitative data. European regulations set no quantitative target, and instead define processes that must be implemented, forcing the industry to adopt a standardized technique to tackle a dynamic problem (payment fraud) and therefore mandating a wooden approach towards security. Mandating a technique or a process does not guarantee low fraud rates. This is even more important in the long-term since fraudsters' abilities are continuously evolving and adapting to fraud prevention technologies and processes. Regulators should set the quantitative objectives they aim to achieve instead of defining the solutions or means to achieve the goal itself, taking into consideration the different risk profiles of the e-commerce industry. Setting metrics (e.g., chargeback rate, fraud rate) indicating an acceptable level of risk or fraud – which could potentially be lowered over time – will both guarantee consumer protection and stimulate innovation and competition.

1. Online payment security: Strong Customer Authentication vs. Targeted Authentication

i. Factors to ensure a high level of security over time

In order to ensure that certain actions are performed by the legitimate card or accountholder, it is necessary to verify the legitimacy of the person attempting to perform such action before allowing its execution. Where the action is performed online, a user willing to perform a transaction to transfer funds from someone else's account or use someone else's payment card (i.e. a fraudulent/ illicit transaction) will need to be able to act as if he were the legitimate user. This may be possible if the system interacting with the user authenticates him as if he were the legitimate user willing to perform that transaction. Authentication is therefore critical to ensure that only legitimate users are allowed to perform transactions, while execution of transactions attempted by non-legitimate users should be denied.

So what exactly is authentication? Authentication is a process whereby the card or account ownership of a user is verified by means of providing certain information to the validating agent, where the information is assumed to be known exclusively by the legitimate user and the validating agent. The authentication process may be based on different procedures and use either a single piece of information or credential, or a combination of credentials. The authentication process is defined to be *strong* when based on a combination of at least two mutually-independent credentials.

Authentication credentials are categorized as:

a. ***Knowledge***: something the user knows
b. ***Ownership***: something the user possesses
c. ***Inherence***: something the user is
d. ***Behavioral***: something reflecting known or expected user behavior

*Credentials categorized as **knowledge** include:*

Passwords and PINs: A password is a finite string of alphanumeric characters used to authenticate a user or access approval to gain access to a resource, while a PIN (Personal Identification Number) is simply a numeric password. Passwords and PINs are often entered after a userID, uniquely assigned to a particular user to access a computer system. A common method to increase password/PIN security is to limit the number of guesses. Original passwords/PINs are disabled and required to be reset after a few consecutive bad guesses (e.g. 3-5). In addition, the user may be required to change the password/PIN after a larger cumulative number of bad guesses (e.g. 20-30) to prevent an attacker from making an arbitrarily large number of bad guesses by interspersing them between correct entries from the legitimate user.

Identifiable images/pictures: A user may be authenticated through images in lieu of a password or PIN to gain access to an online account. The idea behind the use of pictures is that the system shows multiple pictures, and access to the account is granted if the user selects the correct set and sequence of images/pictures. De Angeli et al. (2005) shows that using identifiable pictures for authentication purposes can reduce the ability of non-legitimate users to guess the sequence that will grant access due to leveraging on image recognition abilities of humans. A few banks are beginning to integrate pictures as part of their customer authentication systems, such as Bank of America (Nowell, 2005).

Knowledge-related credentials are static and provide a weak level of security since they may be easily and quickly violated both physically through shoulder, video camera and keystroke sniffing as well as logically via man-in-the-middle and brute force attacks.

*Credentials categorized as **ownership** include:*

e-Tokens: e-Tokens are electronic objects encapsulating user credential data/information. e-Tokens also referred to simply as tokens and may be available in different form factors such as smart cards and USB keys. A token contains user identity information, as if it were a password or PIN, that allow access to restricted resources. A USB token needs to be plugged into a computer USB port so that the computer can process the information stored in it. Software licensing information may be stored on e-tokens to allow proprietary software to be used easily. This makes it convenient to take into account pieces of information such as legal and financial records. Software vendors leverage this specific feature when using e-Tokens to distribute software licenses and check their expiration dates and contractual terms and conditions. It is only when the token is inserted into the computer USB port and the system can access the information contained in it that the authentication process may begin, which implies a hardware check in addition to a logical verification.

One-time passwords (OTPs): One-time passwords are used to allow access to a system during a login process and to other applications that require user authentication. The technique accepts a code, usually generated by a piece of hardware called a token provided by the card or bank account issuer and held by the user, as a valid password that may be used only once. OTPs are

typically generated by time-synchronization or password-concatenation algorithms and verified by a remote server. OTP systems are in fact based on a client-server architecture: the password generator or token (client) must synchronize with/be recognized by the password controller (server) to grant customer access. The dynamic feature of OTPs protects against passive attacks based on captured reusable passwords, which explains its use in online banking. On the downside, OTPs need to be retained and quickly inserted into the correct field and require additional technology to work (an OTP-generating token needs to be distributed to each customer and an encrypted communication network is also required), which may not always be available to users (e.g., an OTP solution relies on the assumption that the user always has his token or mobile phone – in case of an OTP solution based on a text message –, and that the necessary connections are uninterrupted).

Relying on devices as a credential and means to deliver/receive OTPs has drawbacks: devices may be lost, stolen or broken.

*Credentials categorized as **inherence** are biometric credentials.*

Different from credentials categorized as knowledge and ownership, biometric credentials are unique sets of individual traits and, as such, may not be transferred between individuals, stolen, misplaced, lost or forgotten. Whenever individual traits are measurable characteristics, they may be used for authentication purposes.

Biometric credentials include *physiological* and *behavioral* characteristics.

Biometric physiological characteristics are relatively stable physical features, unalterable without causing trauma to the individual. Examples include:

- *Fingerprints:* patterns found on the fingertip, including the location and direction of ridge endings and bifurcations;
- *Hand geometry:* shape of the hand including height and width of bones and joints in the palm and fingers;
- *Patterns in the retina:* layer of blood vessels in the back of the eye.

A number of authentication solutions are commercially available today; however, some are not as robustly secure as commonly perceived (e.g., a fingerprint becomes easier to violate once coded in strings of data), while others (e.g., retina pattern recognition) are very expensive to implement as well as uncomfortable and intrusive for users (Schlenker, Sarek, 2012).

Biometric behavioral characteristics have some physiological basis but also reflect individuals' psychological qualities. Examples include:

- *Signature dynamics:* measurement of a combination of appearance, shape, timing and pressure during the writing of someone's signature;
- *Voice verification:* tone, pitch and cadence of voice;
- *Keystroke dynamics:* the duration of each key-press and the time between keystrokes, speed of keystroke, style of writing capital letters, frequency of errors;
- *Mouse dynamics:* measures mouse movement distance, speed and angle during the work.

Biometric behavioral characteristics are typically less obtrusive than physiological ones and usually do not require special,additional hardware in order to capture the necessary biometric data. Several commercial authentication solutions require limited hardware investments, although software is required to elaborate the captured behavioral information.

Biometric behavioral characteristics reflect individual-specific traits and as such are extremely difficult to replicate by whoever intends to violate a system pretending to be a legitimate user. They include a large number of individual unique characteristics detectable through a few parameters that synthesize them but also retain their uniqueness. Moreover, since behavioral characteristics are uniquely linked to an individual they cannot be assigned to a different person by a third party or even by the customer himself as if they were PINs or tokens.

*Credentials categorized as **behavioral** include:*

- *Customer device:* Each customer may register one or more devices typically used to shop online, which may be checked to spot unusual behavior;
- *Customer type:* Loyal clients are better known so they may enjoy an easier checkout while first-time shoppers may need to take a different authentication path;
- *Location:* The customer geographic position may be monitored via the IP address, mobile signal tracking and GPS of the registered customer device used through an online session;
- *Time to delivery:* Rush-orders, e.g., to be delivered tomorrow may require dedicated authentication paths;
- *Industry-specific characteristics:* E.g., specific airlines routes combined with time to departure may spot suspicious behavior;
- *Shopping behavior:* Online payment and purchasing behavior of a customer may be checked though a variety of parameters including transaction characteristics, currency used, merchant typically frequented, type, frequency and typical amount of purchase;
- *Browsing behavior:* Monitoring changes in email address, changes/addition of new payment instruments, billing and shipping address;
- *Merchant:* Regular transactional behavior at a particular merchant may be monitored by checking parameters including type of items purchased and transaction type as well as fraud performance history.

Behavioral credentials are dynamic as they evolve over time. They offer the opportunity to build and continuously improve the accuracy of a customer profile at every session, creating a self-updating, moving target and erecting a robust and effective barrier to cyberattacks violations.

Credentials may also be grouped into two categories:

1. Credentials that allow static user verification only;
2. Credentials that allow both static and continuous user verification.

The concept of static verification vs. continuous verification is of great relevance in online security. In fact, regardless of how complex it may be to violate a combination of credentials, static verification only allows for user authentication 'at the front door', i.e. when entering a system. Once into the system a non-legitimate user may be able to perform a number of actions as if he were the legitimate user. Although a number of online service providers (including online PSPs) now require customer authentication through an additional piece of credential to authorize the logged-in user to perform a single critical action – e.g. a fund transfer, paying for a purchase, editing customer details – here credentials are used as 'access tokens'. In the event the logged-in user is unable to provide the correct credential(s) when attempting to perform a particular action/ transaction he may continue to access other pages on the website despite potentially being a non-legitimate user that may have accessed a restricted area. Therefore, static verification solutions, while valuable, offer only partial protection against misappropriation of payment methods since they are unable to detect a change in user after the initial authentication.

Continuous verification on the other hand provides protection throughout the entire session. This may be achieved by leveraging behavioral-type credentials through a combination of user interactions with the system during the online session which allows for monitoring customer behavior. Behavioral credentials are dynamic and therefore useful in preventing online fraud. In addition, they can be monitored by the system in the background without requiring customer intervention and therefore have no impact on customer experience.

An example of online fraud prevention that use risk assessment based on behavioral factors leverages location coupled with a time factor. Service is denied whenever a customer logs-in from a location –say London–, and then logs-in from Tokyo one hour later, since it would be physically unfeasible. Another example that leverages a customer's device is to require further customer verification when a customer logs-in from a device different than the one he usually logs-in from. In addition, if the customer attempts to buy goods for a significantly higher amount than his

typical purchase and/or in an unusual currency then the system will signal that the shopping behavior deviates significantly from what is expected for that customer and he may be asked for additional authentication before the transaction is executed; an additional layer of security that effectively mitigates risk and prevents fraud.

ii. Why Strong Customer Authentication is only one secure customer authentication technique and circumstances in which it is appropriate

Strong Customer Authentication (SCA) is defined by the EBA as a procedure based on the use of two or more credentials categorized as *knowledge*, *ownership* and *inherence* (as defined above). In addition, at least one credential must be non re-usable, except for inherence. SCA requires customers to actively intervene in the authentication procedure, thus shifting attention from the purchasing experience.

In general, each technique authenticates customers in its own ways. A category of techniques implements authentication processes/procedures commensurate to the potential risk posed by each attempted transaction. Due to this adaptive/targeted approach we will refer to them as Targeted Authentication (TA) techniques.

The most secure TA techniques dynamically assess the risk of each attempted online transaction by an analytical engine that monitors in real-time a combination of customer credentials, including behavioral factors and transaction characteristics. In addition, the algorithms feature self-learning capabilities so that the actual risk associated with each transaction is continuously updated by monitoring customer activities during each session. This allows for challenging online payment attempts according to their associated risk and, on that basis, the execution of each transaction is either allowed or denied. TA therefore focuses on a) appropriately challenging higher risk transactions requiring appropriate customer intervention aimed at authenticating transaction attempts deemed risky, and b) lighter customer interaction if little or no risk is involved.

The choice of a preferred authentication technique should be based primarily on fraud protection, while we suggest that customer experience should also be taken into account in order to limit abandonment and unnecessary friction.

Real life cases provide useful guidance. Most UK card issuers now use TA techniques and have been implementing them for a few years. They were used to offer traditional 3D Secure authentication solutions that challenge each transaction regardless of their associated risk. The targeted approach focuses on authenticating online payment transactions according to their characteristics and ultimately the associated risk. According to a recent Visa Europe case study on UK issuers implementing TA, approx. 95% of transactions are assessed as low-risk and transparently authenticated with no need for customer intervention, while higher risk transactions (5%) are appropriately challenged and require customer interaction that may differ based on the assessed risk. Approx. 0.2% of transactions are assessed as highest risk and declined because deemed very likely to be fraudulent. The use of TA resulted in no increase in fraud levels as compared to the previously offered 3D Secure authentication solutions, which challenged each transaction with customer intervention (Visa Europe, 2015). This is a noticeable result, particularly in consideration of the very large increase in internet payment volumes occurred in the last few years.

The good performance of TA is mainly due to low false positive rates, i.e. those instances where a transaction is denied due to a suspected fraud when the transaction is in fact regular and non-fraudulent, while actual fraud detection rates are high, and good fraud prevention is achieved. Along these lines, Adyen managed to reduce false positives by nearly 50% with no increase in chargebacks, which in turn increased transaction authorizations threefold (Adyen, 2013).

The cases described show that implementing strong or targeted authentication techniques resulted in the same online fraud rate, so both techniques may be seen as at least equally effective in preventing online fraud. The results suggest that only the higher risk transactions are likely to generate fraud, while the overwhelming majority of the lower risk transactions are genuine and non-fraudulent. Therefore, targeting an appropriate challenge only to the transactions deemed to

have higher associated risk, as opposed to each and every transaction, provides the same high level of fraud prevention.

iii. Practical impacts of mandating SCA

Imposing a rigid process such as SCA on all transactions regardless of their characteristics and associated risk could be detrimental to fraud prevention in the long term. In fact, the robustness of a standard technique or process deteriorates over time, and a regime where no alternatives are left provides no incentive to develop innovative, more effective authentication solutions capable of continuously adapting to fraudsters' abilities.

Mandating a process does not guarantee high security levels to consumers. Since the process is only the means to achieve low online fraud rates, defining the goal itself – a quantitative level in fraud rate – would provide more tangible benefits for customers both at present and in the future. The current regulatory framework does not set any quantitative level in fraud rate to use as a basis for assessing the efficiency of the fraud prevention measures implemented by each provider. We believe an online payment fraud rate (or other metric indicating payment incidents due to potential fraud or unauthorized transactions) against which PSPs' performance could be measured, for example, on a yearly basis, may be an effective quantitative parameter to determine the capabilities of a player to manage online payments risk as well as the effectiveness of the fraud prevention measures deployed. This should be within an official framework so that performance can be applied consistently to all players in the payments value chain –merchants, acquirers, issuers, TPPs– so that the performance achieved by one player is not affected by the performance related to other players.

Allowing PSPs that achieve fraud levels lower than the one set by the regulators the opportunity to rely on alternative customer authentication techniques, possibly in addition to SCA, will provide a strong incentive to limit online fraud. In addition, this will foster the development of innovative fraud prevention solutions that are likely to adapt to changing market conditions, thus retaining the robustness needed to protect from continuously improving fraudsters' attacks and stimulate competition.

Mandating SCA unnecessarily deteriorates customer experience, resulting in higher abandonment due to required intervention – often burdensome – to authenticate each transaction and distract customers from the primary, purchase-related activities. This is a barrier to e-commerce adoption and clearly deviates from the European Commission's objective to stimulate the development of the digital economy in the EU. To illustrate the causal relationship between convenience and conversion, we refer to research showing that optimization of the payment process design and related webpages provides an improved payment experience, resulting in increases in conversion rate of 15% - 20%. In addition, when a more convenient checkout process was implemented on the DeBijenkorf department store website it resulted in fourfold sales, a 50% increase in shopper's time spent on the website, and a 40% uplift in the number of visited pages (Adyen, EDC 2013).

iv. Why Targeted Authentication techniques effectively mitigate authentication risk and why they work well for online payments

The goal of Targeted Authentication (TA) is to focus on challenging transaction attempts with processes and credentials commensurate to the risk associated with each transaction. As a result, transactions with higher risk profiles are authenticated through customer intervention adequate to mitigate the level of risk assessed, while execution of low-risk transactions requires a lower customer involvement, commensurate to the lower risk profile.

TA techniques use real-time monitoring tools and analytical engines that leverage customer behavioral characteristics to assess the risk associated with each transaction and effectively prevent fraud by requiring appropriate challenges on purchasing attempts. Several credentials used by TA techniques are behavioral but often used in combination with credentials that belong to other categories to create a customer profile that reflects their specific behavior. Most

behavioral characteristics are collected during online sessions by monitoring customer interactions with the system, while credentials that belong to other categories are often input by the customer.

Consider a session in which the merchant monitors the location and device-related information associated with the customer's shopping behavioral characteristics[2], feeds that information into an analytical engine that analyzes customer preferences and behavior, and associates that information with the customer's access credentials, e.g. ID and password. Such combination constitutes a very rich data set which identifies a behavioral profile that relates to a specific customer. Customer profiles are stored in a dedicated repository and updated at every online session leveraging the self-learning abilities of the analytical engine. As such, a customer profile is dynamic and therefore extremely difficult to replicate and hence violate, minimizing the residual risk of identity theft. This creates an effectively robust barrier to cyber-attacks. If the customer behavior monitored in real-time during a session deviates more than a preset tolerance level from the profile of the legitimate customer, the system generates an alert and asks for authentication which requires customer intervention. The implemented authentication process will differ and be based on how and how much the monitored customer profile deviates from the legitimate customer profile so that the level of potential risk assessed is adequately mitigated. In the event a fraudster tries to transfer funds illicitly, the transaction will not be executed since the legitimate customer will not confirm the transaction through the required authentication. When the monitored customer behavior falls within the preset tolerance range, the customer is deemed genuine and not fraudulent, no customer intervention is required, and the legitimate customer may execute the transaction seamlessly.

For example, fraudsters are more likely than legitimate customers to make several flat-screen TV purchases from a mobile phone with a card issued in a country different than the one of customer residency on a regular basis while it is common that genuine customers buy more frequently a couple of books and a videogame with their payment method of choice. In this instance TA will detect unusual behavior – and the higher risk – and request the customer to actively intervene to authenticate the transaction. If the customer is purchasing books as usual, the purchasing behavior will match the customer profile and the transaction will be transparently authenticated. Genuine customers will appreciate the request for further intervention in the former situation but a similar request in the latter will annoy them.

Fraudsters are more likely to buy items selling at the highest price. Certain items can also be "high-risk" because of their resale value. Items such as cameras, tickets to games and events, limited edition accessories and clothing, gift cards and jewels are easier to be resold and at higher risk of being purchased fraudulently. Moreover, high value product purchases are approached differently by legitimate customers and fraudsters. Legitimate customers take browsing time checking different models and colors, viewing several pictures of the items and even looking at the e-merchant's guarantee policies. On the other hand, fraudsters show very different browsing patterns. They usually browse the e-shop for a few minutes, sort items from the highest to the lowest price and proceed to checkout with the most expensive items into the shopping cart, with no further browsing. Similarly, it is more common that customers browse 10-15 minutes when purchasing a pair of sneakers to search for the right size and colors rather than buying a dozen designer shoes at once within a couple of minutes, going straight to checkout.

Implementing TA is beneficial to online payments and e-commerce adoption. Both the UK issuers case from Visa Europe and the Adyen implementation described earlier show that fraud is generated by higher risk transactions, while the very large majority of lower-risk transactions is genuine and, as such, they may be transparently authenticated by the system with no customer intervention. This means most customers will be able to fully focus on shopping-related activities such as choosing, evaluating and comparing items without being interrupted, which may result in cart abandonment. In fact, after a customer has gone through the whole purchase process the

[2] Shopping behavioral characteristics related to a specific customer include, but are not limited to: average transaction amount, frequency of purchase, merchant categories, merchant name and payment methods of choice including virtual payment cards

worst possible scenario would be to make it difficult to conclude his shopping and finalize the purchase.

TA techniques implemented by several UK card issuers resulted in a 70% reduction in abandonment compared to the previous application of 3D Secure solutions that required customer intervention for every transaction. The significant reduction in customer abandonment was due not only to the ability to transparently authenticate the majority of transactions – assessed as low risk – but also to the 85% reduction in payment checkout time (from over 50 seconds to 10 seconds) with respect to standard 3D Secure solutions (Visa Europe, 2015).

Paragraph 7.5 of the final EBA guidelines provides scope for merchants and acquirers to manage transactional risk through appropriate detection and profiling. This allows merchants with strong risk assessment capabilities to be able to require different authentication processes for each transaction based on their perceived risk. In practical terms they will be able to implement Targeted Authentication techniques that transparently authenticate transactions assessed as low risk and require customer intervention for transactions with higher associated risk. It should be noted that the EBA guidelines allow this for card payments only. Although card payments account for a large percentage of online payments, that is not the case in some European countries. Since transactional risk is effectively assessed by leveraging a combination of behavioral customer characteristics and does not depend on the means of payment, we recommend this scope to be extended to other online payment methods.

2. Impact of strict security regulations on the digital economy

i. The effect of mandating 3D Secure

3D Secure (3DS) is an XML-based protocol designed to be an additional security layer for online card payments. 3DS adds an additional authentication step in online payments. In its initial form, 3DS would pop-up a password entry form to a cardholder who attempted an online card payment; the cardholder would input the password and, if correct, would be returned to the merchant website to complete that transaction. Difficulties arose with pop-up blockers and now the recommended mode of operation uses inline-frames (*iframe*). The merchant passes the card number to the payment scheme and gets back a URL to embed in an iframe to be displayed to the customer. If the customer executes the protocol successfully, the merchant gets an authorization code to submit to his bank.

3DS solutions authenticate cardholders when they are attempting to execute a payment transaction, i.e." at the door" and in some cases require registration of a static password with the issuer. A standard secure method would be to deliver the password to the customer's address, but in most cases issuing banks require the cardholder to create his own password online on his first attempt to shop online using his 3DS-enabled card, namely an activation during shopping (ADS). The process poses security issues due to the use of static passwords and is not compliant with the EBA guidelines on SCA. Mainly for that reason, issuers are working with solutions providers to replace static passwords with OTPs to comply with new regulations.

While 3DS was designed to strengthen cardholder authentication through real-time verification requiring an additional layer of password authentication, 3DS specifications covers only the communication between the Acquirer Domain (the merchant and the acquirer), the Issuer Domain and the Payment Scheme Domain (hence the name 3 Domain Secure), while customer verification is left to the issuer. As there is no standardization among banks, each one has its own customer experience and verification criteria. To authenticate the cardholder, some issuers require the ATM PIN to be entered, which is also used to authenticate CHIP&PIN card payments at POS terminals; this is to say that cardholders are asked to input their PINs at random e-commerce websites as customer verification procedure is often an ADS process, an unsafe online behavior (Anderson, Murdoch, 2010).

a. Online fraud in card payments: transactions authenticated using 3D Secure vs. using Targeted Authentication

The latest report on card payment fraud issued by the French central bank[3] reports the increased penetration of 3DS-enabled cards issued by French issuers, well over 90% in 2014. Also the report mentions that the share of card payment value authenticated via 3DS increased by 12% during 2014 while during the same year online card fraud rate experienced by cards issued in France increased 2.9 bps from 30.3 to 33.2 bps, or 9.6%.

One would expect a positive impact on fraud reduction due to the increase in transaction value authenticated via 3DS, but these data seem not to support this. Recent experiences highlight that transactions authenticated using TA techniques that focus on appropriately challenging higher-risk transactions show the same level of fraud of 3DS-authenticated transactions (Visa Europe, 2015; Adyen, 2013).

In some cases, implementation of Targeted Authentication resulted in higher fraud protection than previously used 3DS solutions. This was seen at Deutsche Postbank Group in Germany, where a newly introduced TA technique reduced fraudulent transactions by 85% and eliminated support costs associated with 3DS enrollment (MasterCard,2013).

TA allows to focus on challenging the transactions identified as potentially risky, while those with low-risk associated are transparently authenticated. As such, most users that are in fact legitimate customers performing regular, non-fraudulent transactions enjoy a seamless online shopping experience, while potentially risky transactions are challenged to block unauthorized behavior. Here the additional authentication may impact customer experience more than traditional techniques that require customer intervention to authenticate all transactions regardless of their risk profile. This is appropriate due to the potentially higher risk of these customer behavioral and transactional data combinations.

b. Abandonment within card payments: transactions challenged using 3D Secure vs. using Targeted Authentication

Merchant participation in 3DS is mostly not mandatory, but merchants that implement the program benefit from a significant liability shift, as they are no longer responsible for fraud-related chargebacks; instead, these become the responsibility of the issuing bank.

Despite this strong incentive, merchant adoption of 3DS services since its inception in the early 2000's has been much slower than expected. In fact, where enrollment is voluntary, a large percentage of cardholders opt out: e.g. in the USA as many as 52% of users opt out of 3DS at enrollment, while another 18% close the activation window altogether. Even in countries where participation in 3DS is required (e.g. Maestro cards in the UK) 20% of cardholders opt out of the activation during shopping and choose to enroll at a later time. Each cardholder opting out of 3DS when prompted to enroll is experiencing inconvenience due to the enrollment process, eventually leading legitimate customers to abandon purchases due to dissatisfaction (MasterCard,2011).

On the other hand, TA techniques eliminate the need to enroll the customer and challenge only transactions identified as potentially risky. This begins with an assessment of transactional data aimed at identifying where a transaction is being initiated. The assessment is similar to identifying the e-merchant Point of Interaction (PoI) Internet Protocol (IP) data (both device-specific IP and IP geo-location data) of the device on which the transaction is being conducted, and provides useful insights into the history of the customer and the location from where the transaction originates. Along with the use of device fingerprinting via cookies, flash objects and other methods of unique identification, the following questions can be answered: "Where is this customer coming from, and has it been seen before?". Of particular benefit is the ability to compare a current transaction against a historical database of confirmed or suspected elements of fraud across a broad population. This comparison answers the question: "Has this device or customer been associated with fraud before?".

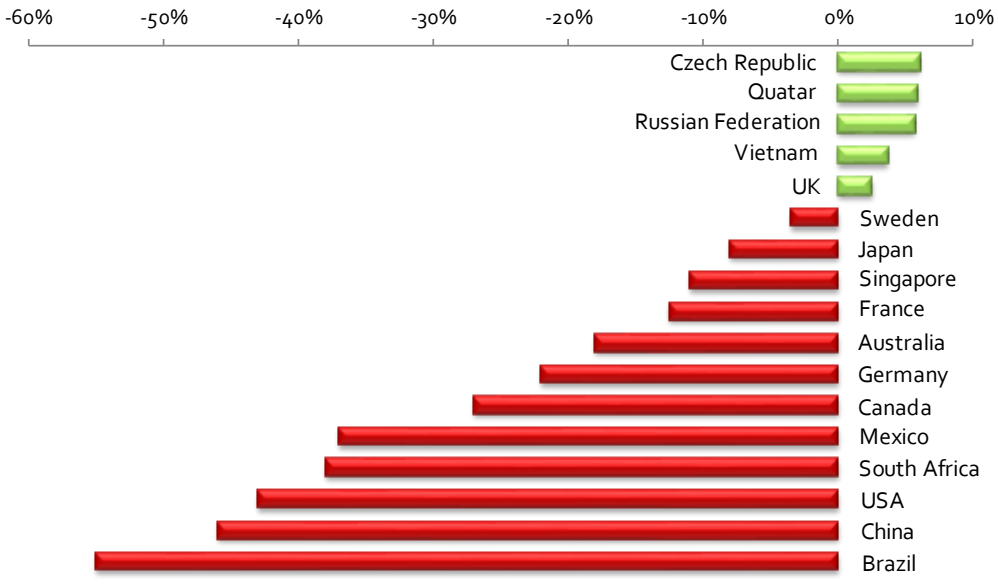
[3] Observatoire de la sécurité des cartes de paiement 2014

This data will then be filtered with behavioral analysis of common parameters, including currency of the transaction, frequency of customer shopping, typical purchasing amount and if the type of purchase fits what we would expect from this merchant. All of this data, potentially enriched with behavioral biometric characteristics such as keystroke dynamics, will be fed into an intelligence engine to determine the relative risk associated with a specific transaction. The TA engine assesses the potential risk associated with each transaction and decides whether to further challenge the customer with additional identity verification or allow the execution of the transaction with no customer intervention when the combination of customer behavioral and transactional data is assessed as a low-risk.

Traditionally merchants have deployed 3DS to all transactions or not offered it at all. Recent experience shows that going beyond this binary (yes/no) view by implementing 3DS in a segmented manner to higher risk transactions results in higher fraud mitigation and increased sales. This is due to the reduction of false positives, i.e. rejection of good, non-fraudulent transactions. In fact, false positives negatively impact revenues by denying good customers and have an effect on brand reputation and loyalty. False positives are reduced by implementing fraud scoring engines that generate a score for each transaction based on analysis of combinations of risk-specific parameters to help merchants decide whether to accept, manually review or deny payment transactions. Social network company Badoo implemented this segmented risk-based technique which resulted in a 4% increase in revenue. In addition, after three months of implementation merchants benefitted by a 41% reduction in card refusal rate, from 12% to 7% (Adyen, 2013).

Research from Adyen focused on assessing the impact of 3DS authentication on conversion reports that in many of the countries assessed abandonment rates – when 3DS was mandatory to finalize the purchase with respect to when it was not asked – are well over 25%, with the USA at 44%, China at 47% and Brazil at 55%. Only a handful experienced just a slight increase in conversion, ranging from 2.5% of the UK to 6% of the Czech Republic, partly due to websites selling items sold uniquely by them, thus forcing authentication through 3DS with marginal abandonment.

Figure 4: Impact of 3D Secure on conversion rates



Source: Adyen, 2013[4]

[4] The research also includes India where adoption of 3DS brought an increase in conversion. However, the India experience is misleading and the results are not comparable with those of other countries. In fact, as of 1 august 2009 all cards issued in India must be 3DS-enabled and online payments must be completed using 3DS but this resulted in high cart abandonment. So e-merchants started to accept order online and accept payments on-delivery, so customers did not have to use 3DS. Actual online payments declined as a consequence but the fewer customers willing to pay online were prepared to go through 3DS. So conversion went up hand-in-hand with payments on delivery.

Differences in abandonment when attempting online payments through mobile devices are even larger. Data from merchants deploying Judopay solutions in 2014 saw a decline in payment rates of 6.6% among customers who were not presented a 3DS payment platform, while the abandonment rate during the checkout phase among customers that needed to go through 3DS authentication was 17.4%, over 2.6 times higher (Lee, 2015). This makes TA even more valuable since online payments are increasingly completed using mobile devices (Visa Europe, 2015).

c. Customer resilience to 3D Secure: Mandatory vs. Choice purchases

A share of online card transactions is attributable to sales of items offered exclusively from a particular website, leaving no alternatives. In reference to the 2014 French central bank report on card payment fraud, card payments taken into account include sales of train tickets from national rail service operator SNCF, payments of taxes and fines, sales of cinema and theater tickets, and others services where competition is slow to penetrate. Most of these merchants require 3DS authentication since they are unlikely to lose any sale while liability is shift to the issuer. Therefore, customers must go through 3DS to be able to buy the services they need, which significantly reduces the overall abandonment rate due to 3DS authentication.

Merchants selling products and services that are also offered by a number of competitors are likely to assess more closely potential lost sales vs. benefits of liability shift brought by mandating 3D Secure authentication. Many such merchants choose to absorb potential fraud losses rather than risk the high rates of transaction abandonment that result from an inconvenient shopping experience. Implementing TA techniques is an alternative that is beneficial to all parties involved – customers, issuers and merchants – as they offer an uninterrupted online shopping experience and lower abandonment while at a minimum retaining a 3DS-like fraud level (Visa Europe, 2015; Adyen, 2013; MasterCard,2013).

3. Impact on customer experience under SCA vs. Targeted Authentication environments

i. Customer conversion at checkout

According to a Baymard Institute report, the average shopping cart abandonment rate has been higher than 60% since 2007 and over 68% in 2014, a level that cannot be overlooked. Of all abandonment instances, cumbersome authentication processes account for 25% (Baymard Institute, 2015). Strong customer authentication requires users to intervene in the authentication process by inputting at least two credentials of different categories, one of which must be non-reusable and non-replicable except for inherence. Since inherence-type credentials are often perceived as intrusive they are seldom used, and most SCA processes rely on One Time Passwords. OTPs are usually generated via an e-token or sent via SMS to the customer's mobile device to be input into specific fields in the checkout page to authorize transaction execution.

Implementing this procedure has a negative impact on the customer experience since:

1. the customer is distracted from purchasing activities;
2. some steps in the process are burdensome and pose challenges.

When customers are distracted from the purchasing experience they may not finalize the purchase due to losing focus. Other challenges that customers face in successfully completing the payment when they are required to intervene in the authentication procedure depend on the authentication process and include:

- *Spot the right code:* in the event OTPs are sent via SMS, the OTP is displayed on the customer's mobile device along with other numbers, including the sender phone number, a number to redirect the SMS, and sometimes other specific codes so the customer may be confused as to which is the correct code to input in the checkout page;

- *Input the code into the right place:* once the customer has generated the OTP via the token or he has identified the correct code sent via SMS, he must remember it and then input it in a specific field in the checkout page;
- *Access to the device:* for token-generated OTPs, the customer must have access to his token when he needs to pay for / complete a purchase, which may not always be the case. In the event of OTPs sent via SMS, they must be delivered to a single mobile device number to retain security; if the customer owns multiple mobile devices, he must carry the one enrolled with the PSP otherwise he may not be able to authorize the transaction.

These challenges make customer intervention burdensome and increase abandonment. On the other hand, TA techniques require customer intervention to authenticate only the transactions with higher associated risk. As a consequence, conversion rates increase significantly: over 70% reduction in abandonment (from 4% to 1%) in the Visa Europe case, which include multiple issuers, and 15-20% increase in conversion as reported by the DeBijenkork department web store (Visa Europe, 2015; Adyen, 2013). Increased conversion is due to the high majority of transactions being low risk and, as such, transparently authenticated by the system and requiring no customer intervention. This resulted in higher quality customer experience and reduced checkout time.

ii. Customer ability to navigate the 'add new card' processes

The majority of online purchases are today paid for using payment cards in most European countries. The ability to add one or more payment cards to a customer-specific repository account indirectly improves the online purchasing experience. In fact, at checkout the customer may simply select the payment card of choice in lieu of inserting all card details; or, in the event a default card is set during enrolment, the customer may be able to checkout through a one-click process since he only needs to confirm that he is willing to use his preferred payment instrument which already resides in the system.

Requirements for handling the 'add new card' process should be based on the circumstances:

1. If the customer attempting to modify/add payment information is well known to the PSP (issuer or acquirer) or merchant, the intelligence engine provides a high level of confidence that he is the legitimate customer that owns the account and, in addition, the customer is the cardholder of the new card, then SCA should not be required and the customer should be able to modify/add payment information seamlessly as he is transparently authenticated by the system;
2. In the event that a newly registered customer is adding a new card to the repository account, the exposure to customer behavior of the TA intelligence engine is likely to have been not long enough to collect enough behavioral information to build a robust customer profile. In such situations we suggest to apply SCA to authenticate newly enrolled customers.

Paragraph 2 above describes the process for handling an e-wallet[5] enrollment as per the EBA guidelines, where SCA is required only when a cardholder enters the contractual agreement or the first transaction and not for subsequent payments[6]. We suggest subsequent payments to include payments using card-data on file, i.e. payments for which the merchant stores the customer's card details. PSPs and merchants will be required to strongly authenticate newly enrolled customers who could enjoy a higher quality customer experience in all subsequent purchases completed using the registered payment instruments that will be authenticated through TA. This will allow one-click purchases that positively impact conversion, in particular by loyal customers who generate repeat purchases, and provide appropriate fraud safeguards. Experiences at a large ticketing operator and a company in casual gaming show that implementing one-click payments

[5] The EBA defines Wallet solutions as *"solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants"*

[6] Paragraph 7.6 of the EBA guidelines states that *"For the card payment schemes accepted by the service, providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data"*

resulted in higher conversion in both cases and incremental sales of 55% for the ticketing operator and 25% for the casual gaming company (Adyen, 2013).

4. Impact on innovation

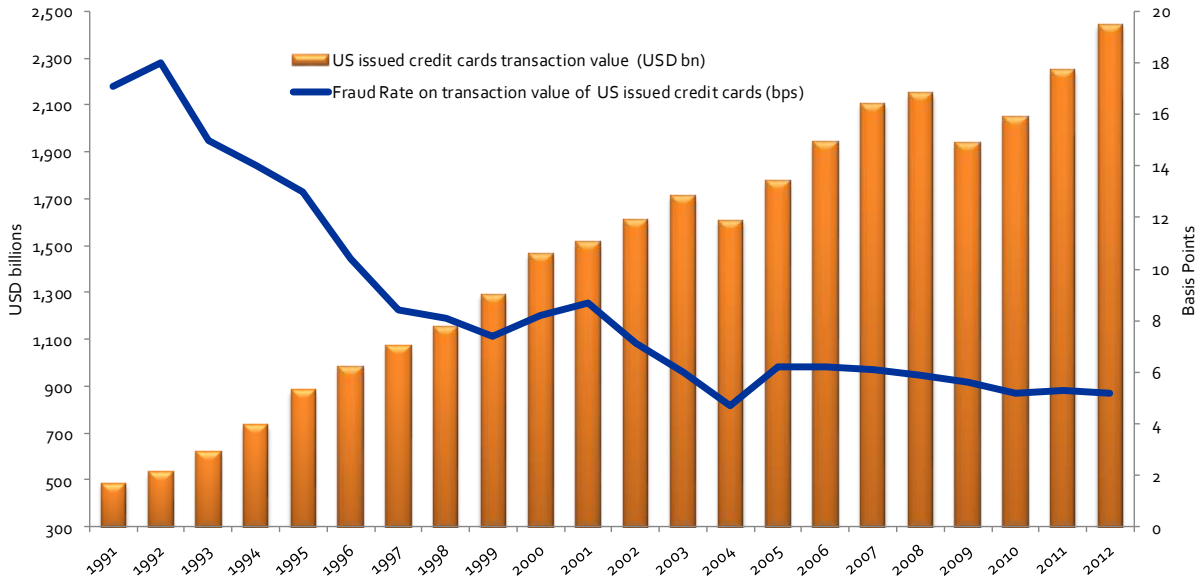
i. How a less strict online environment provides more customer choice and value by promoting innovation and stimulating differentiation and competition

In our view an environment that provides opportunities for all players to offer innovative solutions fosters best-in-class answers to market needs. As such, we support regulatory guidance in setting performance levels to constantly drive development of innovation toward beneficial solutions and enhancement of consumer confidence and trust, particularly in areas such as online payments where these elements are critical.

A country where some regulatory guidance is present but balanced by a willingness in ensuring a high level of competition is the USA. Some interesting data show the impact of the last 20 years of innovation applied to data analytics and fraud prevention on card payment fraud. Real-time fraud monitoring techniques were first applied to the US payment card industry in the early 1990's and card fraud statistics have been monitored since then.

In 1992 overall fraud value as a share of total card transaction value in the USA was 18 basis points, while 20 years later in 2012 the same fraud rate measure was limited to 5.2 basis points, a 71% reduction. In addition figure 5 shows that although the year-on-year reduction in fraud rate was larger in the first 5 years, real-time fraud detection systems have proved to be increasingly effective and able to constantly improve fraud rates over time as a result (FICO, 2014).

Figure 5: US credit cards transaction value vs. Fraud rate value



Source: FICO, Bank for International Settlements

These positive outcomes were driven by market forces. PSPs (issuers and acquirers), schemes and merchants were allowed to compete in attracting customers and needed to persuade them that paying using their credit cards would bring them some benefits. But to pave the way for card adoption, customers needed to perceive them as secure in the first place. So market players focused on creating innovative fraud prevention solutions aimed at reducing payment fraud. This resulted in increasingly secure card payments.

The significant reduction in payment fraud is mostly due to innovation fostered by a non-prescriptive environment. This allowed for the development of data analytics together with the

development of several real-time anti-fraud applications that leveraged the accumulated intelligence from analysis of customer behavioral data and characteristics of trillions of previous transactions aimed at first determining the likelihood that a transaction is fraudulent before it is executed and, if the potential risk assessed is high, further challenging the customer or denying the transaction. This is possible through applications that run tens of thousands of calculations per milliseconds, which were developed over the past 10-15 years due to investments in payment fraud prevention, triggered by stimuli to competition and a focus on achieving a competitive advantage (MasterCard, 2011).

Since cyber criminals continuously adapt their attacks to break into new anti-fraud mechanisms, the robustness of any rigid technique or process deteriorates over time, and therefore investments in fraud prevention solutions are paramount to ensuring the continuous development of online payments as well as adoption and usage of e-commerce services. Such investments are likely to flow toward less severely regulated environments without strict rules and processes, as this would allow more opportunities to deploy innovative fraud prevention solutions.

5. Insights and Conclusions

i. Evidence, insights and concerns

Our analyses of recent and historical official market data show that the industry has developed the necessary capabilities to manage online risk effectively since online payment fraud rates have been constantly decreasing while online payments value has experienced very high growth. This suggests that there is no need for urgent regulatory intervention to increase the security of internet payments and that market players are implementing increasingly effective fraud mitigation techniques thanks to investments in innovation.

Implementing Strong Customer Authentication as mandated by the EBA and PSD-2 will severely impact abandonment, which is likely to increase similarly to what has been experienced with 3D Secure: even after 10+ years of exposure to the technique the declined payment rates in many countries are well above 25%, with peaks close to 60% (Adyen, 2013).

In addition, the approach taken by the regulators appears similar to that used 15 years ago with 3D Secure: mandating a technique that requires customer intervention in the authentication process for all transactions regardless of the risk involved, instead of defining a quantitative fraud level to achieve. Similarly, mandating a rigid process such as SCA requires customers to authenticate every transactions regardless of the associated risk. In addition a wooden approach to a dynamic problem – such as payment fraud – is likely to result in deteriorated effectiveness in the long term since frausters continuously adapt to fraud prevention techniques.

A targeted approach that focus on fighting fraud where it is actually generated has proven to be a valid alternative. In lieu of requiring customer intervention to authenticate every transaction like SCA, Targeted Authentication techniques assess the risk of each attempted transaction and challenge those with higher associated risk with processes commensurate to the risk assessed. Since lower risk transactions are transparently authenticated based on real-time monitoring of customer behavioral information and characteritics of the transaction attempt, TA has no impact on the purchasing experience of customers very likely to be genuine, which is entirely retained and so facilitates conversion.

TA techniques have been developed over the last 15 years and a number of currently available solutions analyze over 100 indicators and parameters to accurately profile customers and assess the level of risk of each attempted transaction. The effectiveness of TA in mitigating fraud has been proven in a number of cases and in particular applications resulted in the same or better fraud prevention than previously implemented 3DS solutions that challenged every transaction (Visa Europe, 2015; MasterCard, 2013; Adyen, 2013).

The current regulatory framework does not explicitly allow for collaboration between players aimed at achieving their common goal of fighting fraud. A collaborative environment offers an opportunity to improve the ability to accurately assess transactional risk as the volume of

information on customer behavior and transactional characteristics available at the different players complements each other, resulting in more effective fraud prevention.

An important concern relates to the absence of any quantitative outcome set by the regulators. Setting a quantitative target to comply with effectively protects consumers as it guarantees lower fraud rates while mandating a rigid process does not.

We are concerned that mandating SCA as identified by the EBA will not stimulate proper adoption and usage of online services and will prevent a rapid expansion of the digital economy, a high priority objective of the European Commission. In addition, this is likely to slow investments in innovation, prevent competition and ultimately offer worse online payment fraud protection to consumers in the long term.

ii. Suggestions on potential improvements of the current regulatory regime

The recent regulatory framework includes aspects that move toward enhanced security in online payments but offers potential areas of improvements.

One is related to requiring customer intervention for every single online transaction with few exceptions. We agree that SCA should always be an available option, but PSPs should also be allowed to offer alternative authentication techniques. Mandating a strict process leaves no opportunities to invest in fraud prevention solutions – aimed at adapting to continuously improving cyberattacks – resulting in deteriorated online payment security in the long-term. SCA results in a burdensome process which negatively impacts customer experience and ultimately increases online abandonment. This will potentially prevent adoption and usage of digital services and in turn slow the development of a market environment that effectively stimulates the digital economy in the European Union.

As mentioned earlier, a number of sophisticated TA solutions have been implemented and proven their ability to offer the same level of fraud protection as traditional authentication techniques such as 3D Secure. At the same time, these solutions offer a more convenient and faster checkout due to the ability to adapt the active customer involvement in the authentication process to the risk associated to each transaction, which results in a more satisfactory customer experience and higher conversion.

Paragraph 7.5 of the final EBA guidelines provides scope for managing transactional risk through appropriate detection and profiling, although it is limited to card payments. We recommend future guidelines to encourage these methodologies and collaboration between industry players, as they have the potential to increase the effectiveness of fraud prevention solutions in the long term and build an increasingly secure online payment environment. In addition, we suggest to extend the scope beyond card payments since transactional risk assessment leverages customer profiles and not characteristics specific to the payment tool.

Customers should not be liable for transactions authenticated through TA. Liability for unauthorized transactions should be allocated to PSPs (issuers or acquirers) or merchants that fail to support SCA, which we recommend to be always an available option to provide customer choice.

We strongly recommend that regulators set an appropriate quantitative outcome to be met in terms of online fraud rate level against which to measure actual performance. This will be useful in monitoring closely the actual performance of PSPs given an approved and accepted standard is in place so that PSPs will be able to consistently apply it in a practical manner across the industry. A PSP should be allowed to offer alternative authentication techniques – in addition to SCA – if in the previous year it has been able to achieve a fraud rate below the level set by the regulators. PSPs unable to achieve the set performance level must offer SCA as the only available option. This alternative approach to mandating a defined process is focused on achieving a performance level deemed satisfactory, which in turn sets an industry standard that all players should offer. The opportunity to offer authentication techniques with higher potential to retain customer experience only for those PSPs with proven capabilities to achieve the performance level set in the regulation greatly stimulates competition. The set target also provides flexibility to be revised

downward – e.g. on a yearly basis – to further stimulate industry-wide performance and create an increasingly secure online payment ecosystem. In addition, the opportunity for PSPs to show their ability to prevent fraud may also further attract customers and in turn additional investments in innovation, which will result in increasingly robust fraud prevention solutions and ultimately benefit all stakeholders and consumers in particular.

The regulatory framework should include guidelines on building a proper customer authentication framework that could be deployed in addition to SCA, along with suggestions aimed at benefiting from a fraud prevention mechanism that features continuous authentication and self-learning capabilities in customer profiling. This will certainly be helpful to the industry as whole and in particular to smaller players.

Our suggestions outlined in this paper have the potential to encourage an environment that stimulates continuous reduction in online payment fraud and increased adoption of online payment services through innovation and healthy competition, and ultimately foster the development of the digital economy within the European Union.

References

- Adyen (2013) "Optimizing payments to increase revenues"
- Anderson S.J, Murdoch R. (2010) "Verified by Visa and MasterCard SecureCode or, How Not to Design Authentication"
- Bank for International Settlements (BIS), "Statistics on payment, clearing and settlement systems in the CPMI countries" (1991-2014)
- Baymart Institute (2015) "Shopping Cart Abandonment Rate Statistics"
- De Angeli, A., Coventry, L., Johnson, G., Renaud, K. (2005) "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems". International Journal of Human-Computer Studies, 63 (1-2), 128-152
- EBA - European Banking Authority "Final guidelines on the security of internet payments". EBA/GL/2014/12_Rev1, 19 December 2014
- Ecommerce Europe (2015)
- European Central Bank (2015)
- FICO (2014) "20+ Years of Analytics Innovations to fight Fraud"
- Haller, Metz, Nesser, & Straw (1998) RFC 2289 – "A One-Time Password System"
- Lee Daniel (2015). "Cart abandonment rates and 3D Secure", 13 April 2015
- MasterCard (2011) "Advantages for a RBA strategy for MasterCard SecureCode", June2011
- MasterCard (2013) "E-commerce Fraud: protecting data, transactions and consumers"
- Nowell, P. "Bank of America Adds New Online Security. The Associated Press", 13 July 2005
- O'Brien Elizabeth "Securing eCommerce Transactions without Losing Customers", August 2015
- Observatoire de la sécurité des cartes de paiement (2009-14)
- Olzak, "Reduce Targeted authentication costs with behavioral biometrics", 17 January 2007
- Payvision (2014), Tackling Internet Payment Security
- Schlenker A, Sarek M. (2012) Behavioural biometrics for Targeted authentication in biomedicine. European Journal for Biomedical Informatics, 8 (5): 19-24, 2012
- Smetters D.K., Grinter R.E. (2002) "Moving from the design of usable security technologies to the design of useful secure applications" Proceedings of the 2002 workshop on New security paradigms, pp. 82-89
- UK Card Association (2008-15)
- Visa Europe (2015), SCA Position Paper, 16 November 2015
- Visa Europe (2014), Risk-based authentication case study

CleverAdvice
Via Ferrante Aporti 34
20125 Milano, Italy

T +39 02 39660672
F +39 02 2870768

e postmaster@cleveradvice.eu
w cleveradvice.eu

CleverAdvice