RESPONSE TO THE EUROPEAN CENTRAL BANK – RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

PayPal welcomes the opportunity to share its experience gained from 15 years of successful activity in the payments business. PayPal is firmly established in Europe and fully committed to the further integration of the European market for the benefit of consumers and businesses.

PayPal believes that the availability of secure and user-friendly payments options for online and offline transactions contributes to integrating markets. This in turn will bolster the economic strengths already present in Europe but also develop the economic potential that lies still untapped.

INDEX

CONTACT
Maija Haas
Senior Manager Government Relations EU
PayPal EU Liaison Office
mhaas@paypal.com

PRESENTATION OF PAYPAL

About the company

PayPal was founded in 1998 in San Jose, CA (USA) and acquired by eBay Inc. in 2002.

PayPal is the global leader in online payment solutions with 110 million active accounts worldwide. Available in 190 markets around the world, users can transact and hold balances in 25 currencies. In EMEA, PayPal has nearly 42 million active accounts.

PayPal acquired a licence as an EU credit institution in 2007 in Luxembourg, with the Commission de Surveillance du Secteur Financier (CSSF) as home state competent authority, subsequently passported into EU member states on a freedom to provide services basis.

PayPal enables any individual or business with an email address to securely, easily and quickly send and receive payments online. PayPal's service builds on the existing financial infrastructure of bank accounts and credit cards and utilises a highly advanced proprietary fraud prevention systems to create a safe, global, real-time payment solution.

Key features of PayPal

Trust: PayPal signals trust to participants in online commerce and into payment transactions due to its unique closed-loop business model. This encourages individual customers and also helps small enterprises and start-ups, who might otherwise not enjoy sufficient trust from potential buyers, to grow their business.

Integration: PayPal operates cross-border and cross-currency, and builds on prevalent consumer preferences which typically differ from one country to another. PayPal hence is highly integrative, connecting consumers and businesses irrespective of their location, currency or payment preference.

Interoperability: PayPal is bank/card-neutral and based on the existing regulated banking and card networks, working in co-operation with all major bank and card schemes around the world. This enables PayPal to connect its users across a wide range of available funding sources. PayPal hence embodies a high degree of interoperability, having integrated the most prevalent payment types (direct debit, credit card, credit transfer, prepaid card, invoice, etc). Interoperability follows commercially sound principles while a high degree of operational security and efficiency is sustained for the benefit of users.

Innovation: PayPal actively promotes innovation in a number of ways. PayPal has already launched several mobile payment products and solutions. PayPal supports the success of innovative start-ups, acting as a trust factor and thus opening wider markets. PayPal also operates x.commerce, an open platform for developers and innovators, which provides an effective launch pad for viable innovative business ideas.

Business development: PayPal is an effective business enabler, especially for small businesses and start-ups. Safe payment options and trust are a key feature to successful online commerce, especially cross-border. PayPal connects entrepreneurs and customers in the market by lending trust to the transaction.
Closed-loop: PayPal is an account based, 3-party system, which means that both the payer and the payee have their account with PayPal. Therefore, PayPal has control over both ends of a transaction, i.e. can trace both sender and recipient of a payment, and builds a quasi customer relationship with its users. Together with highly sophisticated risk management practices and effective anti-fraud technologies practices, this closed loop allows PayPal to identify suspicious behaviour (*see figure 1 below*).

Data protection: Consumer privacy and consumers' financial information in particular, must be protected. PayPal never discloses financial information between the payer and the payee. Only the payment and contact information is transmitted, while all financial information is safely held by PayPal only. This also relieves the merchants, as they do not have the extra burden of safeguarding that financial information.

Buyer and seller protection: Consumers must know that any problems with their transactions will be addressed quickly and fairly in a dispute resolution process. It is important to note here that most transaction issues are the result of honest mistakes or poor communication, not fraud. The provision of a protection scheme and dispute resolution procedures not only benefits individual buyers, but businesses also.

Fight against cybercrime: PayPal is strongly committed to fight cybercrime and to co-operate with national and international bodies, such as government agencies or Interpol. This is of particular importance with regard to financial information, in addition to wider concerns about identity theft and privacy. PayPal's effective collaboration with law enforcement agencies throughout the world, to investigate and prosecute financial crime or privacy-related crimes, contributes to successful crime prevention and hence to increasing confidence in e-commerce.

Ecosystem safety: PayPal works as a leader in the Internet security domain to close systemic weaknesses in the ecosystem. PayPal has coauthored key Internet specifications, such as HTTP Strict Transport Security (HSTS), which is designed to reduce the effectiveness of certain 'man in the middle' attacks, DMARC, which improves the integrity of the e-mail system, and others. This expertise and focus is unusual even for Internet companies, and non-existent within financial services.

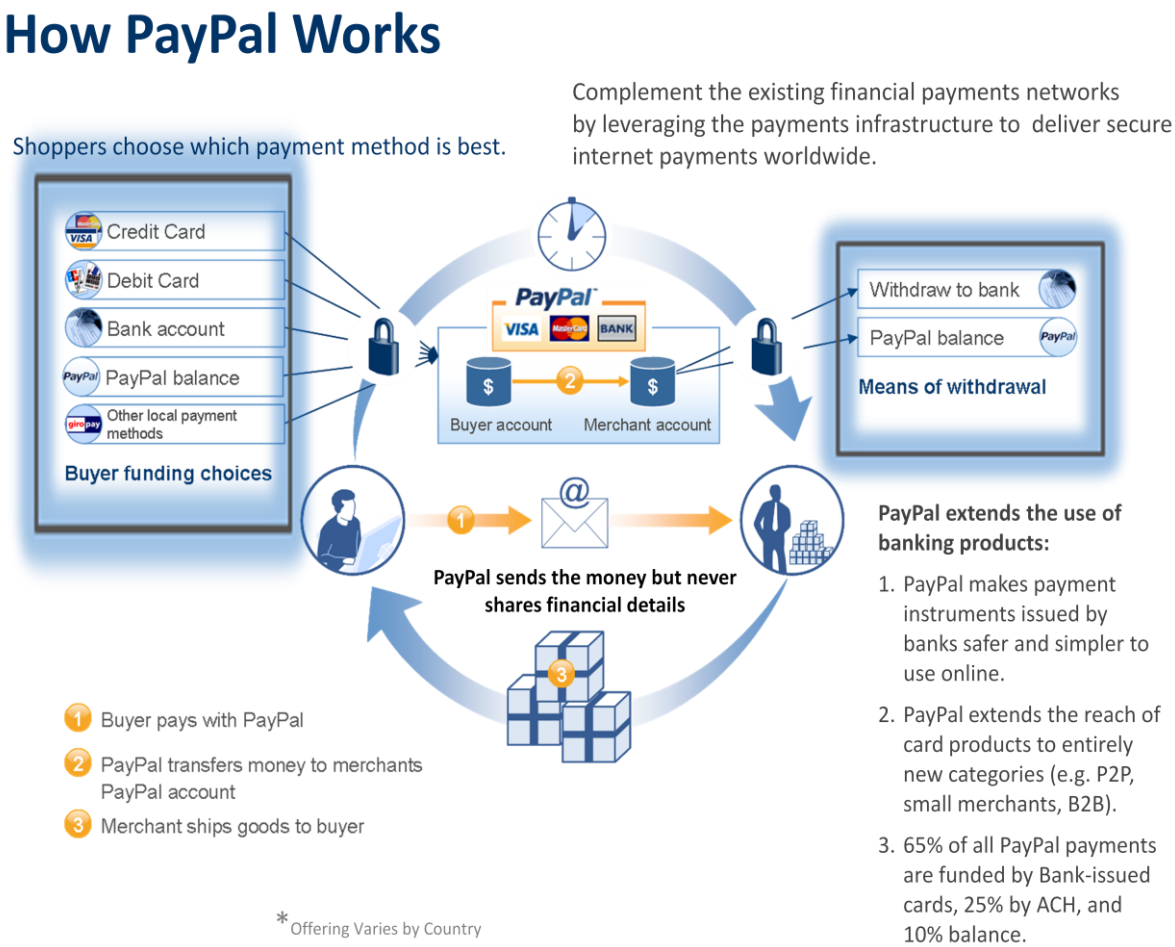
How PayPal Works
Shoppers choose which payment method is best.
Complement the existing financial payments networks by leveraging the payments infrastructure to deliver secure internet payments worldwide.
Credit Card
Debit Card
Bank account
PayPal balance
Other local payment methods
Buyer funding choices
PayPal
VISA
BANK
Buyer account
Merchant account
Withdraw to bank
PayPal balance
Means of withdrawal
PayPal sends the money but never shares financial details
PayPal extends the use of banking products:
1. PayPal makes payment instruments issued by banks safer and simpler to use online.
2. PayPal extends the reach of card products to entirely new categories (e.g. P2P, small merchants, B2B).
3. 65% of all PayPal payments are funded by Bank-issued cards, 25% by ACH, and 10% balance.
1 Buyer pays with PayPal
2 PayPal transfers money to merchants PayPal account
3 Merchant ships goods to buyer
* Offering Varies by Country

FIGURE 1

INTRODUCTION

PayPal welcomes the ECB's objective to foster the establishment of a well-conceived, harmonised EU/EEA-wide minimum level of security through key principles and best practices which will reduce the risk of information and financial loss for the customers of internet payment service providers (PSPs) across the region.

PayPal also agrees with some important principles described in the Recommendations, such as the need to perform specific risk assessments and the adoption of a multi-factor authentication strategy.

However, while security concerns and potential problems must be addressed and met with solid solutions, they must not be allowed to deter business growth and consumer confidence. In addition, security threats are constantly evolving. This situation requires flexible defence mechanisms, which in turn motivate the need for innovation.

In this respect, the security practices listed in the ECB's draft recommendations seem to be based on out-dated techniques and we are greatly concerned that PSPs who fully adopt the recommendations as currently drafted may in fact increase their risk of fraud and customer account compromise, while certainly increasing their operational costs and decreasing their overall transaction volume due to poor customer experience.

PayPal is the world's largest PSP to never suffer a major breach of customer information. PayPal records best-of-class fraud losses while simultaneously setting the industry standard for growth/market adoption through an efficient customer security experience. PayPal is therefore eager to share these insights with the ECB to identify and discourage fraudulent transactions and would like to provide alternative suggestions for an effective and innovative regulatory framework for the ECB to consider as the basis for a review of its recommendations.

WE AGREE WITH SOME OF THE GUIDING PRINCIPLES

- **PayPal agrees with the ECB's recommendation for a multi-factor authentication strategy, which is beneficial as it comes to reducing fraud**.

- **PayPal agrees that payment service providers should perform specific assessment of the risks** associated with providing payment services, as outlined by the ECB. PayPal also agrees that payment service providers should implement effective processes for authorising and monitoring transactions, as identifying abnormal patterns is a key element in preventing fraud.

- **The ECB rightly observes that the constant evolution of technology requires continuous updating of risk assessment and risk management procedures**. While fraudsters may have become more sophisticated, also payment service providers have become more sophisticated in defending their business and consumers against such threats. It is important to note here that commercial interest is a sufficient factor to ensure solid and effective risk management practices of payment service providers.

- **PayPal supports the ECB's declared intention to formulate its recommendations as generically as possible to accommodate continual technological innovation, and not to set specific security or technical solutions**. Such an open, non-prescriptive approach is the most adequate in allowing payment service providers to design and implement effective solutions to ensure continued security in an environment of evolving technology and risk.

BUT BELIEVE THE RECOMMENDATIONS MISS THEIR OBJECTIVE

- **The ECB recommendations focus on the traditional e-commerce environment, where buyer and seller typically do not meet. However, the formerly clear distinction between online and offline transactions is increasingly obsolete**. This change is accelerated by the development of the services available via mobile devices, including payments. The development of mobile commerce and the ensuing amalgamation of formerly distinct commercial channels create obvious challenges for regulators to adequately capture these new models in a legislative framework to enable safe and efficient commercial transactions. PayPal would therefore recommend that the ECB recommendations approach payment security in a more forward-looking manner. This will enable a more comprehensive approach to addressing issues of payment security, independent of the respective channel or platform or method. With a view towards the future of payments, it is important to note that customers may not wish to carry a wallet of multiple payment instruments with different security protocols each when they instead can have all payment options contained in one digital wallet accessible through any device.

- **The recommendations do not take into account the fact that not all payment systems present the same characteristics and expose their customers to the same level of risks**. PayPal for example runs sophisticated risk management systems, which have visibility of both sides of the transaction. The risk level of that type of systems compared to the risk level of single-sided systems is not comparable, so it follows that also requirements for the type and strength of authentication then cannot be the same. Sophisticated risk management systems that reach across both sides of the transaction have a major advantage in detecting fraud and are able to achieve single figure bps loss rates. PSPs with visibility of both sending and receiving accounts can leverage the combination of data associated with both account types to more accurately establish if there is any risk. In addition, when using PayPal, it is not necessary for the customer and the merchant to share financial data in order to complete a transaction. PayPal merchants furthermore increasingly benefit from seller protection, provided they meet certain basic requirements, so that in many cases where a transaction is subsequently confirmed as fraud, the merchant is protected. This largely nullifies the need for additional authentication challenges, setting aside additional customer friction, and enabling smoother ecommerce transactions.

- **In contradiction with the ECB's intention to remain technologically neutral, 3D Secure is clearly presented as one of the best if not the authentication method available.**
  - By detailing 3D Secure in Annex 3, and referring to it as "the architecture for cardholder authentication via the internet" the recommendations can be understood as implicitly endorsing universal adoption of 3D Secure as the sole or preferred architecture for payment service providers, and inadvertently conflating a federated protocol for cardholder verification with an authentication

method. PayPal therefore suggests removing these references to 3D Secure in order to avoid such confusion in the ECB's final publication. Alternatively, PayPal suggests adding at least two more examples of other commercially available multi-factor authentication.

- It should also be clarified that 3D Secure does not by itself ensure strong authentication, since it is simply a discovery service protocol that leverages a registry of authentication end-points. The recommendations include only a very brief acknowledgment of this in a footnote in Annex 3.

- **We disagree with the ECB's definition of strong customer authentication for a couple of reasons:**
  - **The ECB's definition of strong authentication does not address the real issue which is malware.** The ECB assumes that a token-based (i.e. "something you have") One-Time Password (OTP) plus a Personal Identification Number (PIN, i.e. "something you know") authentication meets the definition provided for "strong customer authentication". Yet common forms of malware exist in the ecosystem today that compromise both authentication methods by exploiting just one vulnerability, thus failing to meet the definition provided by the ECB ("*the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s)*"). This threat is increasingly common and there are numerous families of malware which are specifically designed to subvert precisely this condition.
    Malware poses a highly complex and multifaceted risk, and requires flexibility by payment service providers to react adequately to the challenge. If a single security solution or particular authentication method is imposed by regulation, it will in effect facilitate attacks by malware as key elements of all security systems would be well-known and identical. The Transaction Authorisation Number (TAN) in Germany offers a good example of unintended consequences of relying on a specific second factor authentication scheme. The TAN was an early effort by German regulators to raise minimum security practices for online financial transactions. As the market hence focused on this specific authentication scheme, also organised crime successfully focused on circumventing this specific scheme. Although no statistics have yet been shared by the Bundeskriminalamt (BKA) on the overall effectiveness of the TAN strategy in Germany, media have provided substantial anecdotal evidence of this scheme's ineffectiveness to withstand organised criminal attack.[1] PayPal therefore encourages the ECB to solicit the BKA's experience with TAN-based two-factor authentication.
  - Recurring examples of successful attacks on 3D Secure systems highlight the fact that sophisticated fraudulent attempts can subvert the effectiveness of authentication systems that are deemed 'strong' in the conventional sense, which is also applied by the ECB. In fact, we are not aware of a single example of a PSP in EU/EEA operating a security practice **that would actually comply with the definition provided by the ECB**.

- **The recommendations endorse multi-factor authentication, but omit the most effective, future-proof authentication factor: "something that is consistently associated with the user".** Using this fourth authentication factor in combination with back-end risk-based authentication capabilities, a PSP can deliver a truly innovative customer security experience that is built to survive a systemic compromise of any particular authentication factor.

[1] The most recent example was reported just last month; see "Trojan stealing money in German online banking scam" -- http://www.sytech-consultants.com/blog/2012/trojan-stealing-money-in-german-online-banking-scam .

- **The ECB's approach to strong authentication would lead to a commercial reality which is not conducive to a positive customer experience and hence to e-commerce activity**. Introducing excessive authentication requirements is not only disproportionate to the actual risk of harm to the customer, but it also introduces hurdles to customer sign-up which would negatively impact on commercial activity. The consequence is that customers are unlikely to complete registration and engage in transactions. This would stifle the development of e-commerce rather than promote its growth, and hence completely contradict the policy objective of the European Commission. It would also put Internet payments, mobile payments or other innovative forms of payments at a commercial disadvantage as compared to traditional payment methods. This would create an unjustified and anti-competitive imbalance as regards investment, consumers experience and market access for e-commerce.

WE WOULD LIKE TO SUGGEST AN ALTERNATIVE FRAMEWORK

We strongly encourage the ECB to promote the use of back-end risk-based authentication capabilities. These capabilities allow PSPs to dynamically select the most effective authentication challenge for any given authentication context. The benefits of this approach are twofold: (i) the context assessment measures are difficult for fraudsters to understand and attack, and permit nimble responses to an ever-changing threat landscape and (ii) it is customer-friendly.

Risk-based authentication capabilities are not the same as standard fraud monitoring. Most anti-fraud monitoring capabilities are initiated after an authentication event. Risk-based authentication is the ability to leverage a variety of factors, including but not limited to device recognition, in a combinatorial scheme that is spoof-resistant and highly effective when combined with one or more shared secrets.

We also suggest making use of innovative authentication factors to better achieve the ECB's objective of strong customer authentication.

Example: Comparison of a PSP's commitment to using SMS OTP as its second authentication factor to a multi-factor authentication strategy relying on back-end risk-based capabilities.

By relying solely on an OTP sent to a consumer using SMS or MMS as the second factor, the protection is only as reliable as the connection between the consumer and her phone number, for every transaction. Leveraging instead on back-end risk-based capabilities, such as recognition of the consumer computer (one of many assessment tools for establishing a trust score for the authentication context), along with occasional use of SMS authentication when users enrol a new computer as a strongly authenticated trusted device, will significantly improve protection and reliability as the end user is successfully recognised as long as she either has access to either the same computer or phone as previously used.

This approach also simplifies user experience and permits the addition of other user-facing security measures. If there is reason to suspect the phone number is compromised, risk-based authentication capabilities enabled with a multiplicity of authentication challenge would enable the PSP to simply use another authentication challenge instead.

PayPal would therefore like to present an alternative, forward-looking framework for a harmonised minimum level of security best practice that will reduce the risk of information and financial loss for PSP customers.

One core element of such an innovative framework is an **alternative definition of strong customer authentication**, based on the ability to empirically protect the customer from harm. Another central feature is the **fourth authentication factor which leverages current and emerging technologies to assess "something consistently associated with the user"** (aka "something you do"). This requires **back-end risk-based authentication capabilities** to make dynamic decisions concerning the most effective authentication techniques in any particular authentication context. It also highlights the need for PSPs to invest in innovation as regards authentication challenges so as to fend off organised crime.

As the ECB considers single-factor authentication, as only control mechanism, inadequate for transactions involving access to customer information or movement of funds to other parties, PSPs should use effective methods to authenticate the identity of the customers using their products and services. The authentication techniques employed by the financial institution must be appropriate to the associated risks of harm to the customers. **Financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks**.

A regular risk-assessment update is of utmost importance given the speed of technological progress. PSPs should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services
  - Identifies risk mitigation actions, including appropriate authentication strength
  - Measures and evaluates customer awareness efforts
- Adjust, as appropriate, their information security program in light of any relevant changes in technology, sensitivity of customer information, and internal/external threats to information.
- Implement appropriate risk mitigation strategies

The use of two or more of the following elements categorised as knowledge, ownership, inherence and associative information is required:

- something only the user knows, e.g. password, personal identification number
- something only the user possesses, e.g. token, smart card, mobile phone
- something the user is, e.g. biometric characteristic, such as a fingerprint
- something that is consistently associated with the user, e.g. using the same device from the same location, or how they type their password/move their mouse, et al.

In addition, the strong authentication procedure should be designed so as to mitigate the risks related to the confidentiality of the authentication data. This must be in combination with back-end risk-based authentication capabilities which enable a dynamic selection of the appropriate authentication challenge, based on a dynamic risk assessment of the respective authentication context.

The framework set out above is informed by our own multi-factor authentication strategy and makes extensive reference to the revised guidance for authentication in an internet banking Environment, published in 2011 by the Federal Financial Institutions Examination Council (FFIEC).

The fundamental difference as compared to the ECB's current draft recommendations is the emphasis on PSPs' ability to react to changes in the risk environment by introducing new authentication methods. The burden of proof lies on the PSP to demonstrate their techniques effectively mitigate the risks of harm to the customers.

It would be beneficial as regards effectiveness and coherence of all applicable regulatory guidance and recommendations to align the ECB recommendations with other existing and applied guidance such as the FFIEC's, especially keeping in mind that the e-commerce environment is global and will achieve its greatest potential for economic growth and integration only if the existing regulatory barriers can be overcome.

Other more specific amendments to the Recommendations could include:

Amendment 1: Risk Based Authentication

[Pg 5] *'. Second, as an outcome of taking a risk based assessment of a transaction, ~~as a general principle~~ the internet payment services provided by PSP's ~~should~~ may be initiated by means of the most relevant strong customer authentication.*

This will enable PSPs to conduct an adequate risk assessment of a transaction or account event, and to determine the appropriate response. It may lead to the use of a traditional 2 factor authentication challenge, but this is not mandatory. Alternative challenges may be considered if they provide the same level of confidence, or even a higher degree of confidence in the user's authentication.

Amendment 2: Alternatives to 'Strong Authentication'

[Pg 6] *'…Where the recommendations indicate solutions, PSPs may achieve the same result through other means. This flexibility extends to the definition of strong authentication. PSP's may adopt an approach which captures the characteristics of a transaction, including its originator and its destination, derive multiple authentication factors from these, and using rules and/or models assess the risk of the transaction being fraudulent. The output of the risk assessment determines the routing of the transaction to mitigate the perceived level of risk, which should result in the most relevant authentication challenge to the customer.*

This insertion counters the narrowness of the current definition of strong authentication. It allows PSPs to adopt a multi-factor authentication without the imposition of all the restrictive elements of strong authentication such as dongles, tokens etc. Customers may still choose to adopt that level of security, but it should not be mandated upon the PSP to use these if they have adequate, safe alternatives.

Amendment 3: Compensatory measures

[Pg 6] *'...Where the recommendations indicate solutions, PSPs may achieve the same result through other means. It is recognised that PSPs have to balance the need for imposing strong authentication routines (as defined in the ECB 'Guiding Principles' pg 6) alongside the impact such processes have on the customer experience of using the service and the impact of inappropriate levels of friction, such as checkout abandonment. Accordingly, it will not be mandatory for PSPs to implement strong authentication (as defined in the ECB 'Guiding Principles' pg 6) so long as internet transactions are subjected to alternate risk based assessment routines that have an acceptable level of efficacy in detecting fraud. The burden is on the PSPs to demonstrate the ability of their systems, and for the regulator to provide an objective benchmark that the PSPs perform to.*

This ensures that the performance level of various approaches towards delivering security in transactions is reached, without mandating approaches that may not be relevant to PSPs due to the maturity of their risk management systems. It also avoids developing of such payment service propositions where user experience would be frustrated by the imposition of an outdated, limited definition of strong authentication.

COMMENTS ON OTHER SPECIFIC RECOMMENDATIONS

Recommendation 4: Risk control and mitigation

PayPal points out that there is already a requirement on Payment Service Providers to require merchants to implement security measures to protect customer data.

The international card brands created the Payment Card Industry (PCI) Security Standards Council. The PCI prescribes a set of technical and operational standards on any merchant or payment provider that store, process or transmit cardholder data. PayPal complies with the standards and also participates directly on the Council given that PCI security is recognised as a collaborative rather than competitive issue.

The standards apply different requirements on different constituents in the payment market. They also use a commercial risk-based approach which recognises that sophistication and investment will differ between sole proprietors, small and medium business or large multinational corporations. The standards are then enforced by the card schemes.

Merchants can however choose to circumvent these requirements by allowing a PSP to host their payment page or by not requiring their customers to pass them their financial details.

Recommendation 6: Initial customer identification information

PayPal notes that the ECB recommendation here creates a conflict with the EU Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (AML3).

AML3 in fact allows simplified due diligence (SDD) in certain cases, which include e-money transactions below certain qualifying thresholds. It means that e-money issuers may defer customer verification until certain activity thresholds are reached. SDD has since proven to be adequate, and PayPal therefore warns against creating confusion for customers and businesses by putting this Directive into question.

From an economic point of view, removing SDD, or lowering the relevant activity thresholds would introduce a major hurdle for consumers at the very initial phase of commercial transactions. This would lead to a drastic reduction of e-commerce activity and reverse the successes that services providers as well as merchants have achieved until now. The economic cost of on-boarding customers would hence outweigh the risk investment and lead to drastic decline in business activity.

If it is the objective of EU authorities and regulators to encourage and increase e-commerce, especially cross-border, it is crucial to build on the existing agreements which have proven to function well in the market, not to dismantle the conditions for business activity.

Recommendation 9: Log-in attempts, session time-out, validity of authentication

PayPal agrees with the ECB that payment service providers should limit the number of authentication attempts, define rules for payment session "time out" and set time limits for the validity of authentication. PayPal has all relevant mechanisms and procedures in place and confirms their effectiveness.

Recommendation 10: Transaction monitoring and authorisation

PayPal fully supports the recommendation to conduct transaction monitoring in real time and according to specific screening and evaluation procedures.

Harmonised categorisations for authentication messages may however be difficult to implement in practice. Firstly, it creates continued practical problems as any such categories would have to be changed whenever a merchant changes their product type or service. It is not evident that a rigid regulatory categorisation requirement would correspond to the commercial reality of an evolving market. Secondly it would impose significant cost to set up and maintain such a harmonised categorisation. This may not be commercially viable for many service providers. The example of large merchants in particular, selling a wide range of diverse products illustrates that such a categorisation would not be practical. Only a very wide categorisation could apply here, in itself defeats the underlying idea of specification.

Recommendation 11: Protection of sensitive payment data

PayPal believes that the EU regulatory framework achieves the right balance of robust data protection and of providing space for innovation in the development of payment products and related technology.
PayPal fully agrees that payment authentication methods must be compliant with data protection requirements. PayPal also endorses the access restriction to authentication data only to directly and necessarily involved parties as an effective requirement to ensure data protection.

Another measure to ensure adequate data protection and privacy is transparency about the mechanisms in place, as this increases service providers' accountability. This transparency must be clear to customers of the service on the one hand to increase trust in the payment transaction, and on the other hand securely anchored in corporate governance principles.

PayPal does not agree with the suggestion that payment service provider should assume responsibility for e-merchants' data handling, which would be an overexpansion of applicable data protection legislation. It would be neither justified nor feasible in practice to comply with such an obligation or recommendation.

Recommendation 12: Customer education and communication

PayPal fully agrees that customer education is key element in payment security. In order to ensure that also customers themselves become more sophisticated in using payment services, and in recognising potential risk factors, PayPal fully endorses the ECB's call for engagement in customer awareness and education programmes on security issues.

PayPal contribute to consumer education on security risks, for example by regularly communicating its customer base on how to handle suspicious emails. PayPal also offers other methods to provide assistance and guidance on the secure use of internet, and also mobile payments, including public awareness campaigns and co-operation in various industry associations and regulatory working groups.

But while we do a lot in this area, we believe Member States authorities could and should do more to educate customers with both remedial outreach to the general public and the development of specific primary and secondary school Internet safety and security curricula.

Recommendation 13: Notification, setting of limits

PayPal strongly opposes the imposition of restrictive requirements on internet payments which do not apply to other types of payment services.

Payments are services at the disposal of customers, which can be carried out via a number of means. In addition to being commercially not viable, there is no justification why internet payments should be subject to specific limits which do not apply to other payments. Any such tendencies would amount to clear discrimination between internet payments and others, and run counter to the EU's objective to encourage e-commerce and innovative payment solutions.

Furthermore, not all internet payment systems are the same and therefore do not all present the same kind and degree of risk. Limits should not therefore be imposed arbitrarily but must take into account the specific structure of the particular system.