CA Viewpoint

Summary of EBA Guidelines and How CA can Help

To: Payment Card Issuers
From: The CA Technologies Digital Payments Product Team
Subject: Meeting the EBA Guidelines and EU Payment Security Directive for secure authentication
Date: 3 February 2015

The European Banking Authority (EBA) recently published *Final Guidelines on the Security of Internet Payments*[1] outlining the minimum Internet commerce security standards that card issuers must implement by 1 August 2015. These guidelines are based on the regulations set out in the EU Payment Security Directive (PSD) and will incorporate forthcoming Payment Services Directive (PSD 2) when released to ensure consistent Internet payments service adherence across the 28 EU Member States. The bottom line for card issuers is the requirement to adopt a multi-factor, defense-in-depth authentication approach to support internet card use by 1 August 2015.

The importance in combatting fraud losses is underscored by the increase of card-not-present fraud in 2012 by 21.2% over 2011[2]. In support of the fight against payment fraud, EBA core requirements are centered on strong customer authentication[3] and aim to increase consumer trust in Internet payment services. The EBA Guidelines present issuers with best practices and by following these Guidelines issuers can protect customer data and ensure that the rightful user, not a fraudster, is initiating a payment. Guidelines 4, 5, 7, 8, 9, 10, and 13 bear particular scrutiny regarding implementation of a multi-factor authentication solution. These recommendations include:

- Implementing a cardholder authentication solution, such as 3D Secure (3DS), for internet use
- Incorporating multiple layers of "defense in depth" security
- Using fraud detection and prevention technology to identify suspicious transactions
- Ensuring that a strong authentication solution is enabled for high-risk card-not-present cases.

The 14 specific EBA guidelines are summarized as follows:

1. Implement and regularly review a formal security policy
2. Carry out and document thorough risk assessments
3. Ensure consistent and integrated monitoring, handling and follow-up of security incidents
4. Incorporate multiple layers of security defenses
5. Have processes in place that ensure all transactions are properly traced
6. Identify customers and confirm their willingness to make internet payments
7. Protect internet payments, as well as access to sensitive payment data using strong customer authentication[3]
8. Ensure that customer enrolment and authentication provisioning is carried out in a secure manner
9. Limit the number of log-in or authentication attempts and session length
10. Operate transaction monitoring tools to prevent, detect and block fraudulent payments and subject high risk transactions to specific screening and evaluation before the transaction is completed
11. Protect sensitive payment data when stored, processed or transmitted
12. Provide assistance and guidance to customers and communicate the authenticity of messages received
13. Set limits for internet payment services and provides customers with options to further limit risk including alerting and profile management services
14. Confirm the payment initiation and provide customers "in good time" with information to verify a payment is legitimate.

In reality, payment card issuers must balance the necessity for secure Internet payments and protection of cardholder data along with maintaining a smooth, user-friendly cardholder experience. CA Technologies offers comprehensive software solutions that allow issuers to meet and exceed some of the EBA guidelines and be ready for the potentially more stringent PSD 2 regulations – solving for secure customer-friendly internet payment experiences. See Appendix A for more detail.

How CA Technologies Payment Security Products Meet EBA Requirements

As a leading provider of Internet payment security solutions, CA Technologies is the ideal partner for issuers to smoothly meet the 1 August 2015 deadline. By implementing an easily customizable CA Technologies payment security cloud service, issuers can achieve a powerful card-not-present payments foundation, create a seamless customer experience, and meet the requirements set forth in the EBA strong authentication guidelines.

CA Transaction Manager our 3DS service, is used by over 13,500 portfolios with over 150 million active cardholders worldwide.[4] More issuers are choosing CA Transaction Manager everyday because it enables a dynamic and personalized online shopping experience. And, because our payment security product team has been involved with developing 3DS technology since initial establishment of the secure protocol, CA Technologies can provide seamless 3DS compliance with

Verified by VISA®, MasterCard® SecureCode, JCB J/Secure™, American Express SafeKey® and Discover/Diners ProtectBuy℠ cardholder authentication programs.

CA Risk Analytics is a "Zero-Touch" authentication cloud service that uses advanced statistical predictive models and dynamic rules to assess the potential risk of each transaction and instantaneously deny, alert, allow, or require additional authentication for each transaction appropriately. No explicit cardholder interruption occurs during the checkout process unless additional verification is triggered based on the scoring results.

CA Strong Authentication provides simple, intuitive and dynamic authentication that fully meets the EBA definition of strong customer authentication. Offered on-premise or as a cloud service, CA Strong Authentication can provide an alert to the cardholder for confirmation that it is a valid transaction. Using **"**2-way notification," transactions identified as potentially fraudulent can be validated instantaneously by cardholders allowing them complete their transaction or identify it as fraudulent. This versatile authentication solution enables multiple authentication modes including a 2-factor soft credential, OTP delivered via SMS or voice, Mobile OTP application, 2-way notification and other multi-factor options.

What does this mean for Current CA Technologies Payment Security Customers?

The increasing sophistication of fraudsters and the desire for an improved customer experience has already led a significant number of CA Technologies customers to choose our solutions. We are confident that very little effort will be required by current users of our eCommerce solutions to fully comply with the EBA definition of strong authentication. Customers can quickly enhance their products by working with us, but the following outlines some initial considerations.

If you are using:	Then upgrade to:	Rationale:
CA Transaction Manager	CA Strong Authentication	CA Transaction Manager customers who currently use static passwords alone for 3DS authentication should consider immediate deployment of CA Strong Authentication to meet the EBA requirements with a variety of options including a 2-factor soft credential; OTP via SMS, voice, email; Mobile OTP generator, and 2-way notification and transaction verification.
CA Transaction Manager & CA Strong Authentication	CA Risk Analytics	Good news! By using CA Strong Authentication, you can meet the EBA requirement for strong customer authentication. However, we recommend adding CA Risk Analytics to improve the customer experience. This provides a frictionless checkout experience for genuine cardholders and only suspicious transactions will require additional authentication.
CA Transaction Manager & CA Risk Analytics	CA Strong Authentication	CA Risk Analytics can identify and block suspicious transactions. However, you will still need CA Strong Authentication to meet the EBA Guidelines for strong customer authentication to verify the genuine cardholder.

We are committed to work closely with CA customers and partners to fully deliver solutions that increase customer loyalty, grow revenue, and ensure compliance with the higher security standards required under current and future regulations.

What's next?

Stay ahead of the 1 August 2015 implementation deadline — Contact us today! We can advise you on what CA Technologies payment security products may suit your needs and work with you to implement the best secure authentication options as you prepare for the regulatory deadline.

Learn more about CA Technologies Payment Security Products at www.ca.com/ecommerce or send an email to paymentsecurity@ca.com to connect with a product expert. CA Technologies customers can contact their account representative for a detailed assessment on how our payment security solutions fulfill the EBA Guidelines on the Security of Internet Payments and EU Payment Security Directive (PSD) regulations.

[1] See http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
[2] See http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf
[3] For the purposes of the EBA Guidelines, strong customer authentication is defined as a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.
[4] Source: CA Technologies data 4th quarter of calendar year 04.

Appendix A:

	EBA Guideline	Solution	Application of CA Technologies Payment Security Solution
1	Implement and regularly review a formal security policy	Internal Bank policy	Using CA Risk Analytics, issuers can dynamically customize fraud and risk policies settings according to individual financial institution policies.
2	Carry out and document thorough risk assessments	Internal Bank policy	Issuers can use authentication data from CA Risk Analytics to augment risk assessments.
3	Ensure consistent and integrated monitoring, handling and follow-up of security incidents	Internal Bank policy SIEM Solution	
4	Incorporate multiple layers of security defenses	CA Transaction Manager CA Risk Analytics and CA Strong Authentication	The combination of these products will allow you to meet the requirements for strong authentication and transaction monitoring achieving "Defense in Depth" for internet payment transactions.
5	Have processes in place that ensure all transactions are properly traced	CA Transaction Manager CA Risk Analytics	CA Transaction Manager implements 3DS so that each transaction can be authenticated. CA Risk Analytics provides additional authentication data and an audit trail for each transaction. Case Management capabilities provide "true" fraud data.
6	Identify customers and confirm their willingness to make internet payments	Internal Bank policy	
7	Protect internet payments and access to sensitive payment data using strong customer authentication[3]	CA Transaction Manager CA Strong Authentication CA Privileged Identity Manager (PIM)	CA Transaction Manager implements 3DS so that each transaction can be authenticated. CA Strong Authentication provides multiple options for multi-factor authentication including OTP via SMS, Mobile OTP app, 2-way notifications for both internet payments and access to sensitive payment data. CA PIM provides through fine-grained user access controls, shared account password management, authentication bridging and user activity reporting–in both physical and virtual environments for privileged user.
8	Ensure that customer enrolment and authentication provisioning is carried out in a secure manner	CA Strong Authentication	Provides secure enrolment, FYP, and de-provisioning workflows.
9	Limit the number of log-in or authentication attempts and session length	CA Strong Authentication CA Single Sign-on (SSO)	With CA Strong Authentication, issuers can choose limits for authentication attempts. CA SSO can incorporate logins from multiple channels.
10	Operate transaction monitoring tools to prevent, detect and block fraudulent payments and subject high risk transactions to specific screening and evaluation before the transaction is completed	CA Risk Analytics	CA Risk Analytics provides real-time analysis of each transaction, applies advanced 3DS authentication models, and produces a score that identifies both legitimate and high-risk transactions. Dynamic rules allow you to apply customized business policies.
11	Protect sensitive payment data when stored, processed or transmitted	Internal Bank policy CA products do this for the data we manage	CA Technologies maintains secure, Payment Card Industry (PCI) compliant, SSAE 16 audited eCommerce Solution data centers so that data transmitted during the authentication process keeps cardholder data protected.
12	Provide assistance and guidance to customers and communicate the authenticity of messages received	Internal Bank policy	CA Transaction Manager and CA Risk Analytics can support customer service managers (CSM) in determining when a potentially fraudulent transaction has occurred. The CSM can then communication this information to the customer.
13	Set limits for internet payment services and provide customers with options to further limit risk including alerting and profile management services	CA Transaction Manager CA Risk Analytics CA Strong Authentication	CA Risk Analytics can analyze a transaction and determine its level of risk. It can send an alert to customers, request step up authentication or deny the transaction based on bank policies. CA Strong Authentication can send an OTP via SMS, email or Voice, or initiate 2-way customer notification so that the customer can respond immediately to continue a transaction.
14	Confirm payment initiation and provide customers "in good time" with information to verify a payment is legitimate	Internal Bank policy	

[1]European Banking Authority Final Guidelines on the Security of Internet Payments

Press Release
London.UK
Published 19/12/2014 | EBA/GL/2014/12

The European Banking Authority (EBA) published today its final Guidelines on the security of internet payments, which set the minimum security requirements that Payment Services Providers in the EU, will be expected to implement by 1 August 2015. Concerned about the increase in frauds related to internet payments, the EBA decided that the implementation of a more secure framework for Internet payments across the EU was needed. These Guidelines are based on the technical work carried out by the European Forum on the Security of Retail Payments (SecuRe Pay).

Among various measures aimed at more efficient and secure internet payments across the EU, the EBA guidelines require in particular that Payment Service Providers (PSPs) carry out strong customer authentication in order to verify the customer identity before proceeding with an on-line payment, one of the key measures to prevent internet fraud, be it through banking services or internet card payments. These Guidelines, which are based on the technical work carried-out by SecuRe Pay -the voluntary cooperation forum reuniting central banks and supervisors of Payment Service Providers -, will be applicable to all PSPs across the EU in a consistent manner as of August 2015.

The EBA decided to issue these Guidelines because of the rising levels of fraud observed in internet payments. Latest pan-EU figures showed that fraud on card internet payments alone caused €794 million of losses in 2012 (up by 21.2% from the previous year). A timely and consistent regulatory response was therefore needed while waiting for the revision of the Payment Services Directive which aims at creating a more secure, competitive and consumer-friendly rules for payments in the EU.

Geoffroy Goffinet at the EBA Consumer Protection Unit explained that: "the EBA guidelines on internet payments provide the legal basis for achieving a level playing field for all PSPs across the EU. Through this piece of work, the EBA looked into supporting the development of e-commerce across the EU, while ensuring proper protection of consumers."

PSPs will also be required to provide assistance and guidance to their customers in relation to the secure use of internet payment services. In particular, they will have to initiate customer awareness programmes so as to ensure that their users understand risks and best practices in internet payments.

Regarding consumer data protection, the Guidelines foresee that PSPs offering card payment services to e-merchants should encourage them not to store any sensitive payment data or require that they have the necessary measures in place to protect these data. PSPs should also carry out regular checks and if they become aware that an e-merchant handling sensitive payment data does not have the required security measures in place, they should take steps to enforce this as a contractual obligation or terminate the contract.

All competent authorities across the EU are expected to comply with these Guidelines by incorporating them into their supervisory practices and amending their legal framework or their supervisory processes accordingly.

Note to the editors
These Guidelines will provide a solid legal basis for the security of internet payments across all EU Member States while the revised Payment Services Directive (known as PSD2) is finalised in coming years. A consultation on the implementation of these Guidelines was launched in October 2014.

The EBA work on this topic results from a concerted effort with the European Central Bank (ECB) to increase the security of retail payments and was developed on the basis of the recommendations issued in January 2013 by the European Forum on the Security of Retail Payments (SecuRe Pay). SecuRe Pay was established in 2011 as a voluntary cooperation between supervisors of Payment Service Providers (PSPs) and overseers of payment systems and payment schemes/instruments within the EU/EEA with the aim of facilitating knowledge sharing and understanding of security of electronic payment services and instruments.

Press contacts:
Ms. Franca Rosa Congiu
E-mail: press@eba.europa.eu - **Tel:** +44 (0) 207 382 1772