GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Meeting EBA Guidelines for Internet Payment Security with Mobile-Based Authentication

A Goode Intelligence white paper sponsored by TeleSign

www.goodeintelligence.com

First Edition September 2015

Sponsored by TeleSign

Published by:
Goode Intelligence

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

This white paper from research and consultancy company Goode Intelligence (GI) explores the implications for Payment Service Providers of European Payment Authentication and Security Guidelines. The paper identifies TeleSign as a partner for payment providers in meeting these guidelines through frictionless mobile-based identity solutions.

EUROPEAN BANKING AUTHENTICATION REGULATION

There is a pressing need to deploy strong, agile, authentication technology to ensure that financial and payment service providers (PSPs) can reliably identify legitimate customers and prevent fraudsters and criminals from accessing their accounts. Tackling fraud by letting legitimate customers in, enabling a frictionless payment experience, keeping the criminals out and ensuring that rising levels of online fraud are controlled.

Weak authentication solutions are allowing criminal hacking teams to by-pass security to enact billions of Euros worth of financial fraud. This fact has not been lost on the European Union (EU), with the European Commission (EC), the European Central Bank (ECB) and the European Banking Authority (EBA) responding to increasing levels of financial fraud with the development of standards and guidelines for the use of strong customer authentication for payments.

The EU's response includes the Payment Services Directive II (PSD2) and the EBA's guidelines on internet payment security[1].

The EBA's guidelines were published in December 2014 to provide a "solid legal basis" for the security of internet payments within the EU and Payment Services Providers operating in the EU were expected to implement them by 1 August 2015.

The EBA security guidelines provide PSPs with a minimum set of guidelines to ensure they have a secure framework to protect internet payments against fraud and provide guidance until the revised Payment Services Directive (PSD2) is finalised – anticipated for 2018/19.

So what do the EBA guidelines provide for PSPs in terms of

Goode Intelligence White Paper

GI's white papers offer analyst insight from research extracted from primary sources including surveys, analyst reports, interviews and conferences.

GI Definitions

EC: The European Commission is the executive body of the European Union (EU) and is responsible for proposing legislation, implementing decisions, upholding EU treaties and managing the day-to-day business of the EU.

ECB: The European Central Bank is the central bank for the Euro currency and monitors monetary policy for the Eurozone.

EBA: The European Banking Authority is the banking regulatory authority of the EU headquartered in London.

PSD2: The Payment Services Directive Version 2 is an EU Directive to regulate payment services and payment services providers

PSP: A Payment Service Provider enables retailers to accept electronic

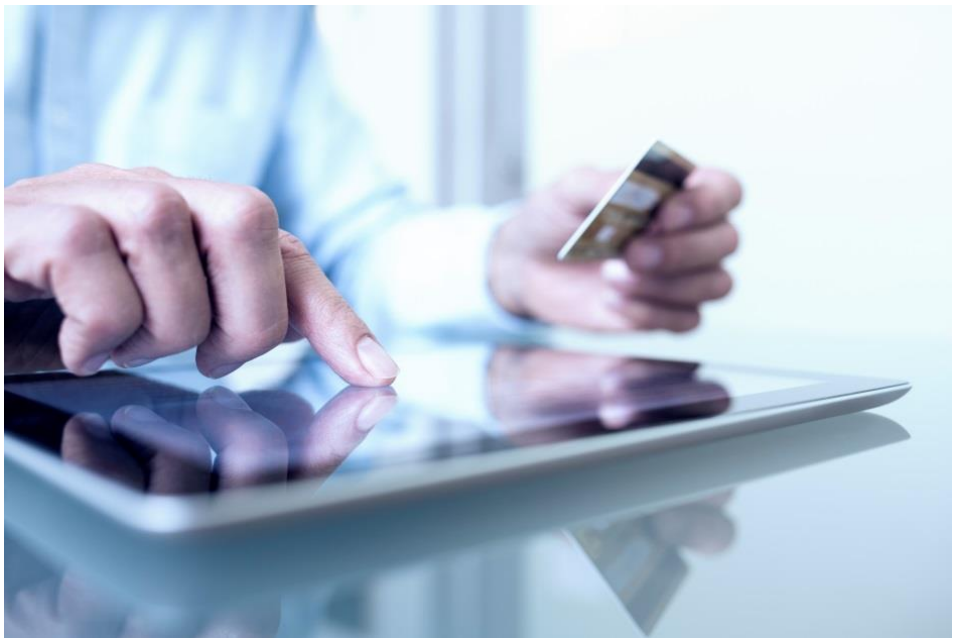
[1] Guidelines on internet payments security, European Banking Authority: **https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments**

appropriate levels of authentication (strong customer authentication)?

payments through a range of payment methods including credit and debit card.

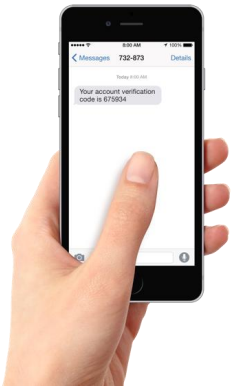
- Defines *authentication* as a "procedure that allows the PSP to verify a customer's identity"
- Defines *strong customer authentication* as a "procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. a 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."
- Strong customer authentication should apply to the "initiation of internet payments" and customer "access to sensitive payment data"

These guidelines do a good job of summarising current industry best-practice for the operation of strong customer authentication but how do PSPs ensure that they choose the right solution that not only meets the guidelines, is suitable across a range of payment scenarios, while ensuring those customers have a good experience?



MEETING THE EBA STRONG CUSTOMER AUTHENTICATION GUIDELINES WITH TELESIGN'S MOBILE IDENTITY SOLUTIONS

It is imperative that PSPs and financial services providers deploy strong customer authentication solutions that meet the EBA's guidelines, prevent attacks and provide a frictionless experience for the customer.



Goode Intelligence believes that a modern authentication solution must meet industry regulation, prevent known attacks and provide a frictionless experience for the customer

A company that has developed strong authentication solutions that meet the EBA secure internet guidelines on strong customer authentication and can also deter common attacks is **TeleSign**. TeleSign has been named as a "Leader" in Gartner's 2014 Magic Quadrant for User Authentication report.

TeleSign's Mobile Identity solutions offer PSPs mobile phone-based authentication and verification that meets the need for strong authentication in a post internet payment legislation world.

TeleSign's unique selling proposition is based upon balancing the needs of payments ecosystem with the needs of the customer; the right balance of regulatory compliance, simplicity and security.

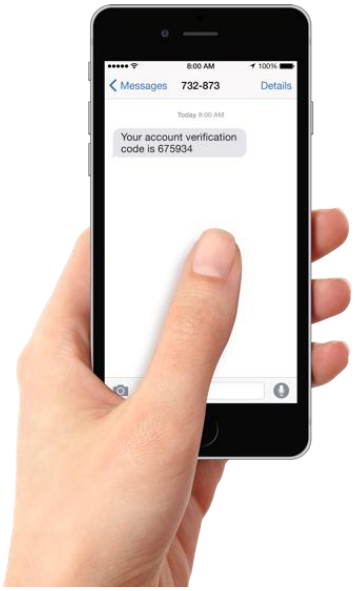
By starting with a unique identifier that is already in the hands of billions of consumers worldwide, the mobile phone and the associated number, TeleSign has created portfolio of authentication solutions that are simple to use and secure. The concept of mobile identity is based on three components: a ***mobile phone number***, a ***mobile device*** and a user's ***mobile activity or behavior***.

Mobile Phone Number

A mobile phone number is something that is rarely changed, with mobile network operators (MNO) supporting number portability allowing customers to assign numbers to a new SIM card on a different network.

Ubiquitous and unique, this makes it one of the best and persistent user identifiers for those operating in the payments industry.

A mobile phone is also a very active identifier as when a phone connects to the mobile network, the MNO validates the number and verifies that the account is in credit and active; also checking that the device has not been lost or stolen. This MNO generated data is a goldmine for identify verification purposes.



MNO: A Mobile Network Operator or wireless carrier is a provider of wireless (cellular radio) communication services.

SIM: A Subscriber Identity Module is an integrated circuit chip that stores mobile subscriber data including the International Mobile Subscriber Identity (IMSI) number and is used to identify and authenticate subscribers.

IMSI: The International Mobile Subscriber Identity is a unique identification number used by the mobile network to identify subscribers.

Mobile Device

The EBA guidelines state that strong customer authentication comprises of “something only the user possesses”. A mobile device is the natural authentication device; always with the owner and generally always on.

Each mobile device has its own unique International Mobile Station Equipment Identity number (IMEI) and has a wealth of additional attributes that can be used to uniquely identify the device.

IMEI: The International Mobile Station Equipment Identity number is a unique number to identity mobile phones and is used by the mobile network to identify valid devices.

Behaviour

The third component of TeleSign's Mobile Identity is behavior, meeting another requirement of the EBA's strong customer authentication guidelines; "something the user is".

TeleSign use mobile network data, including location to build up a profile of user behavioural patterns that can distinguish between a legitimate device owner and a potential fraudster.

TELESIGN MOBILE IDENTITY – THE GO-TO-SOLUTION FOR PSPS

For those operating in the payments ecosystem, TeleSign's mobile identity solution is ideally positioned to provide strong customer authentication.

Online payment fraud, defined as card not present (CNP) fraud, is rising in the UK, CNP fraud increased by 10 percent from £301 million in 2013 to £331 million in 2014.[2]

CNP: A card not present transaction is a payment card transaction made where the cardholder does not or cannot physically present the card at the merchant. This includes online, mail order or telephone scenarios.

Providing a secure and frictionless authentication experience for online payments is essential for PSPs to ensure that fraud levels are within acceptable levels.

TeleSign's mobile identity solutions have proven to be extremely effective in verifying legitimate users and reducing fraud in the online payments experience.

Payment card issuers can easily bind the TeleSign mobile identity to

[2] Plastic fraud figures, The UK Cards Association: **http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp**

the card and ensure online transactions remain secure and are in compliance with EBA's secure internet guidelines on strong customer authentication.

MOBILE-BASED AUTHENTICATION – THE PERFECT PARTNER FOR PAYMENT SERVICE PROVIDERS

The mobile phone is the perfect authentication device. It is packed full of sensors and identifiers that can be leveraged to identify both the device and its owner. Mobile Phones are rarely out of reach from their owners; a survey discovered that three quarters of 25-29 year olds sleep with their phones. [3]

Mobile-based authentication is becoming the de-facto standard for strong customer authentication and is suitable for a wide-range of payment scenarios. The mobile phone can be leveraged for eCommerce payment transactions using the mobile phone as the second factor or within a mobile application through a mobile app software development kit (SDK). By leveraging standard mobile phone technology such as SMS (for the delivery of one-time-passwords) or a voice call, mobile-based authentication provides a cost-effective and scalable solution for payment service providers ensuring customers don't have to carry or find additional devices to verify transactions.

OTP: One-Time-Password. A cryptographically created single use passcode that can be created by hardware or software tokens.

It is not just the mobile device itself that is being used as an authentication enabler. The mobile network can also be leveraged, providing valuable data that can be used as part of an identification process. Using the mobile phone number as a key identifier and a number of data attributes associated to the phone, such as SIM Swap or Call Forwarding detection, payment service providers can be given precise risk scoring for their customer's phone numbers based on network activity. For instance, payment providers can be told if a particular mobile phone number has been used in multiple account registration attempts across a range of eCommerce service providers. They are then able to create specific workflow around this intelligence to either reject the account registration request or to follow-up with further investigation.

From securely validating new customers during account registration to protecting account access and transaction verification, mobile-based two-factor authentication is an essential tool for organisations operating within the payment ecosystem that also care about good customer experience.

[3] Your Wireless Life: Results of Time's Mobility Poll, Time: **http://content.time.com/time/interactive/0,31813,2122187,00.html**

SUMMARY AND CONCLUSIONS

The European Banking Authority's security guidelines provide PSPs with a minimum set of guidelines to ensure that they have a secure framework to protect internet payments against fraud and provide guidance until the revised Payment Services Directive (PSD2) is finalised.

The guidelines provide guidance for PSPs in deploying strong customer authentication technology to combat rising levels of internet payment fraud.

TeleSign's Mobile Identity Solutions meet the EBA guidelines and provide payment services providers with a mobile-based frictionless authentication solution that is applicable across a wide range of payment scenarios. By leveraging devices already in customers' hands, TeleSign's solutions help Banks and PSPs strike balance between cost, risk reduction and great customer experience.

Learn more about mobile-based authentication at **www.TeleSign.com/solutions**

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in information security including:

- Mobile Security
- Authentication and Identity
- Biometrics
- Internet of Things Security

For more information on this or any other research please visit www.goodeintelligence.com.