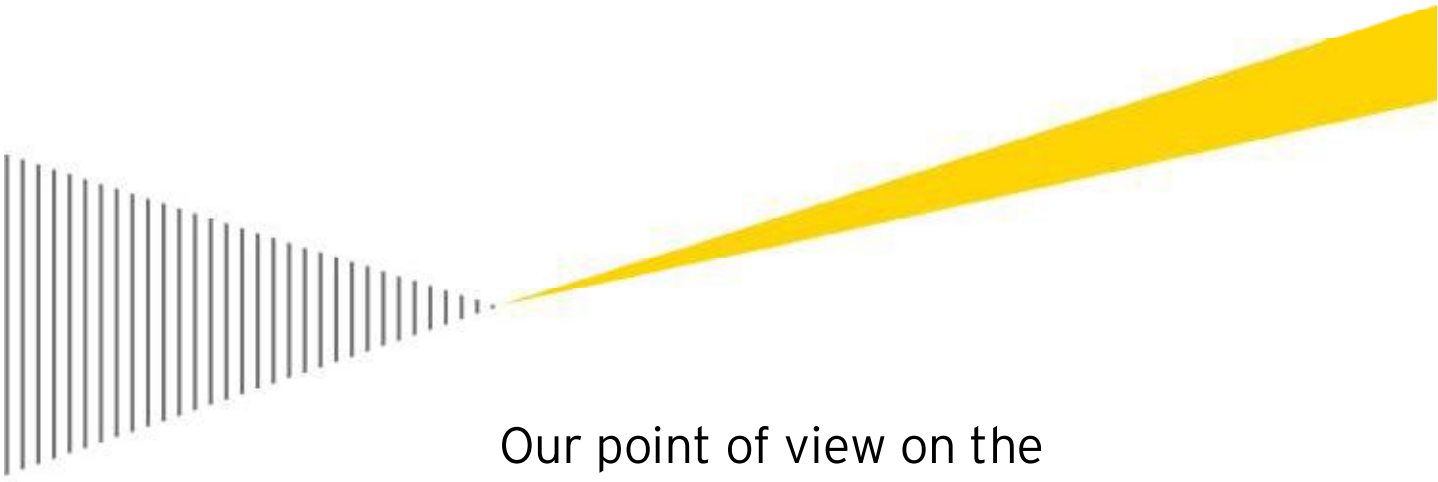
Security of Internet Payments



Our point of view on the 'Recommendations for the Security of Internet Payments' of the ECB

Summary

- Payment Service Providers and Governance Authorities have to prove compliance with latest regulation on the security of internet payments, published by the ECB, by 1 FEB 2015 or earlier.
- The ECB report is a step-up in the EEA/EU wide regulation of internet payments and goes beyond existing regulation or industry standards.
- More regulation (i.e. on Payment Account Access, Mobile Payments and Near Field Communication as well as Information Sharing on Security Incidents) is about to follow.
- The past has shown that national payment regulators were disappointed when they began testing compliance.
- It is essential to understand what needs to be implemented, how this overlaps with existing or additional national regulation and how it can be achieved in an efficient and commercially viable way.

Who is in scope and what is the timeline

In January 2013 the European Central Bank (ECB), fully supported by national authorities, published their final recommendations, key considerations and best practices with regards to the security of internet payments. The ECB report is applicable to all

- Payment Service Providers (PSPs), as defined in the Payment Services Directive Payment Directive 2007 64 EC[1] , providing internet payment services, such as internet card payments, including virtual card payments, as well as the registration of card payment data for use in e-wallet solutions, the execution of credit transfers on the internet, the issuance and amendment of direct debit e-mandates and transfers of e-money between two accounts via the internet, and to
- Governance Authorities (GAs) of payment schemes (including card payment schemes, credit transfer schemes, direct debit schemes, etc.).
- E-merchants will also be affected, as PSPs will have to obtain contractual assurances from them that their systems meet stringent security requirements prescribed in the recommendations.

It is expected that the addressees comply with the recommendations and key considerations as they define the minimum expectations by the ECB. Where they do not comply, they need to be able to explain and justify any deviation upon request of the relevant competent authority ("comply or explain" principle). In addition, all addressees are encouraged to adopt best practices listed in the report.

The recommendations should be implemented by 1 FEB 2015. This only gives organizations 2 years in which to ensure full compliance. National authorities may wish to define an even shorter transition period where appropriate[2].

[1] This includes i.e. credit institutions, electronic money institutions and payment institutions.
[2] The ECB also announced that it will launch a public consultation on draft recommendations for payment account access services.

A step-up in the EEA wide regulation of internet payments

When you read the ECB report you might be tempted to presume compliance with all requirements for your venture – one way or another.

However, the past has shown that national payment regulators were disappointed when they began testing compliance, i.e. with the Payment Service Directive requirements, they were disappointed that a number of firms had no systems in place to check whether they were compliant but instead responded that 'their systems were designed to be compliant'[3]. Some were not even aware that they had to comply.

Sometimes it is important to be reminded that addressees of regulation are asked to provide evidence of compliance and that lacking compliance can result in significant fines, the loss of a license and certainly a massive damage to the reputation.

The ECB report is a step-up in the EEA/EU wide regulation of internet payments and goes beyond existing regulation or industry standards such as the Payment Card Industry's Data Security Standards (PCI DSS). It foresees the stringent implementation of. i.e.

- Strong customer authentication[4] measures for all internet payments
- Multiple layers of defenses and a dedicated and documented security policy framework
- Adequate security tools enabling near real time monitoring, screening and blockage of transfers
- Sound customer due diligence, identification and verification procedures pre account opening
- Clear contractual agreements between PSP and e-merchants as well as outsourcing providers on security standards

- A requirement which conflicts with the market participants focus on customer convenience
- Requirements which currently may not be met by many market participants to the required extend
- Apart from the challenge to implement appropriate procedures, search and successful implementation of technology solutions within 2 years can become a problem
- A requirement that also conflicts with commercial objectives and – if done wrong – could keep customers away
- This means more responsibility for acquirers to monitor and assess their business partners but also for the business partners themselves to comply with the ECB recommendations

[3] See Speech by Sheila Nicoll Director of Conduct Policy at the Intellect/Payments Council "Driving Change in Payments" conference, May 2011.

[4] Strong customer authentication is a procedure based on the use of two or more of the following elements – categorized 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.

What needs to be implemented

In summary, the report outlines expectations regarding general control and security environment, specific control and security measures for internet payments as well as expectations towards customer awareness, education and communication. This includes requirements on:

Governance

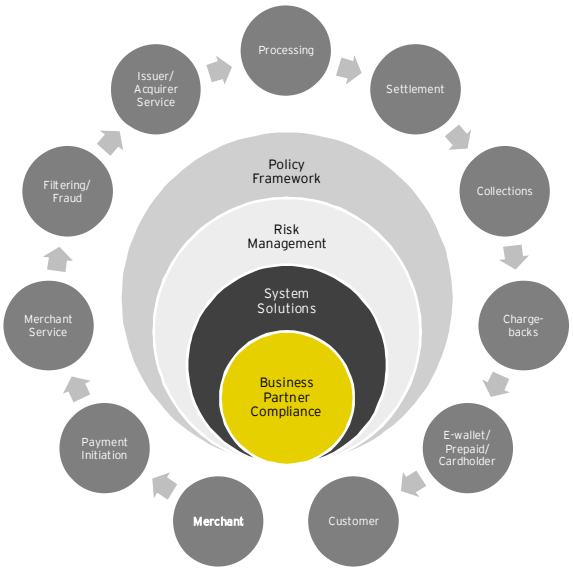
- Definition and implementation of a risk based 'Security Policy' framework
- Implementation of strict internal and regulatory reporting procedures

Risk Management

- Definition of a sound risk assessment methodology with regards to the security of internet payments for customers, e-merchants as well as IT infrastructure and applications
- An annual risk assessment process and definition of risk scenarios
- Risk based strong customer authentication procedures
- Definition and maintenance of sound transaction monitoring rules and screening requirements
- Customer Due Diligence procedures (incl. AML, KYC, CTF relevant components)
- Behavioral analysis
- Multiple layers of security defenses (defense in depth)
- Training to customers, internal staff and e-merchants

Information Technology

- Customer screening solutions
- Transaction monitoring solutions
- Fraud detection systems
- Customer due diligence solutions
- eID&V
- Risk assessment engine
- Customer profiles
- Interfaces to risk monitoring, screening and alert systems
- Traceability
- Customer equipment
- Customer notification / secure channels



Compliance and Audit

- Ensuring compliance of business partners (e-merchants) and outsourcing partners
- Periodical internal and external audits of security measures

Why to start early – check your readiness now and ensure co-ordination

The recommendations by the ECB are showing that the attention of the regulators is increasing nearly at the same rate as the internet payment sector is developing. Whilst it becomes a non-negotiable prerequisite to implement sound operational practices it is important to understand how this can be done best and in time, as:

- The regulator allows a risk based approach
- Multiple methodologies and technologies are available in the market
- Competitors are facing the same challenge and – if done right – the implementation of efficient security measures can become a competitive advantage

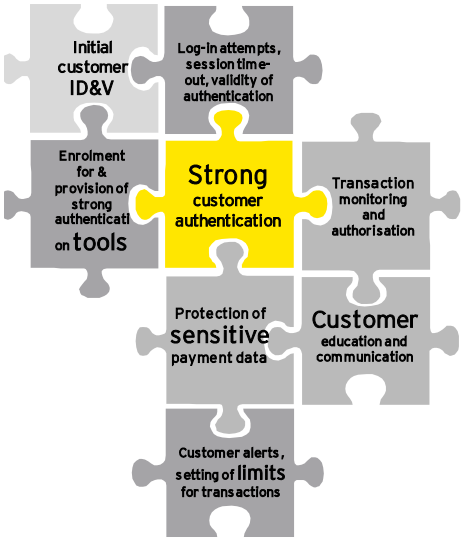
Implementation of these measures requires thorough planning well in advance of 1FEB 2015. Firstly, to allow for the definition of risk based requirements in dialogue with the global and local regulators. Secondly, to allow for the proper selection, implementation and testing of automated and robust system solutions in the wider context. And thirdly, to better co-ordinate ongoing initiatives covering similar issues or simply affecting the same systems and procedures to be changed, i.e.

- SEPA or other implementation activities
- Planned innovation in payments
- Upcoming recommendations for 'Payment Account Access' Services
- Upcoming regulation on 'Mobile Payments and Near Field Communication (NFC)'
- Upcoming regulation on 'Enhanced Information Sharing among Authorities on Security Incidents'

The co-ordination of multiple activities requires a strong and early established Program Management Office that

- Understands, overlays, structures and communicates all relevant requirements
- Phases activities and maps them into the delivery plan of the individual projects
- Flags delays and enables senior management to make quick decisions where conflicts arise
- Produces clear reports and documentary evidence etc.

An early start is inevitable if addressees want to avoid delay, duplicative effort and reputational loss in what becomes a regulated environment. Lessons learnt from the Financial Services sector and i.e. the introduction of SEPA or Risk Management regulation have proven that project cost can increase substantially if done otherwise.



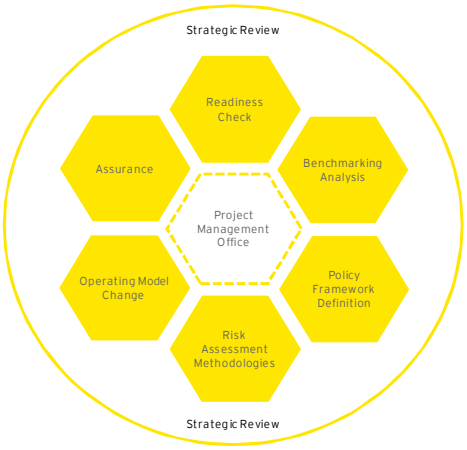
How can Ernst & Young help

Ernst & Young can help you to achieve your potential in what is a changing and increasingly demanding environment. Based on our expertise in the Payment and wider Financial Services Sector we can offer you support throughout the entire implementation life cycle. Our services include:

Strategic Review
As the new and stringent requirements by the ECB can have a severe impact on the market and an individual organization we conduct a strategic analysis together with you including

- Product portfolio review
- Profitability analysis
- Strategic partner review
- Horizontal and vertical value chain analysis
- Customer and colleague impact analysis across business segments

The outcome can help you to understand your position in the market, where you want to generate revenue and where to better divest with regards to complexity and cost of current and future regulation.



Readiness Check

- The Readiness Check starts with a current state analysis where we will review your organization at a detailed level and from an end-to-end perspective. This means together with you we go through the entire process chain and track what you have already implemented i.e. based on your own principles or on other market standards
- Based on the current state analysis results we will conduct a detailed gap analysis, screening each relevant dimension of your organization along the payment service value chain for shortfalls against the new recommendations and their interpretation by local and supra-national regulators
- Defining an optimal roadmap early will help minimize costs, increase flexibility and improve the outcome. We will work with you to design this optimal roadmap, taking into account the broader portfolio of regulatory change, and kick start 'no-regrets activities' now
- The Readiness Check can be applied across the piece or per thematic cluster such as governance framework, processes or IT. As an output you will receive
  - A clear description of your status quo.
  - A clear gap analysis against the new requirements including recommended activities
  - A clear impact analysis of the suggested activities on your value chain.

Benchmarking Analysis

- Comparing your status quo and implementation plans with your peers, allowing Risk Appetite and standing with the regulators
- The Benchmarking Analysis can be conducted as a stand-alone exercise if you have done any of the other elements on your own and want to be re-assured you are within good market practice.

Assurance

- We can provide you with support for the development, implementation or review of a Security Assurance and Control Framework.
- We can also manage the Project Office for you and support you in the co-ordination of your workstreams, whether they are staffed by you, us or others

Project Management Office

- During the mobilization of the program we will work with you to define the appropriate governance structure, reporting requirements and roles and responsibilities for the successful implementation of required changes
- We will help you to establish a strong Project Management Office that ensures that there is
  - Good visibility of program progress across all workstreams/ sub-projects
  - Timely escalation and resolution of risks and issues
  - Rapid and effective decision making by the appropriate people
  - Effective use of management time and key resources given the need to balance implementation of new measures with the requirements of business as usual
- We can utilize and embed a range of tried and tested program management tools. We can also provide you with professional project managers who have done this before for payment service providers and who can lead the overall program, individual projects or workstreams as required

Policy Framework Definition

- In close collaboration with your Senior Management, Risk and Compliance functions, Operations and others we support the definition, documentation and socialization of your dedicated Security Policy as requested by the regulators. Whilst it is a challenge to define a robust but also commercially balanced policy framework it is indispensable to bear its timely implementation in mind. Only if your policies pass the 'use test' they are real.
- Based on our experience in operational transformation and change management we can help you to define sound and practical rules meeting regulatory expectations where you operate.
- We will also help you to understand the impact of the new policy framework on your product portfolio respectively business proposition as if not included at an early stage, it can generate friction between business leads and your security function

Risk Assessment Methodology and Scenario Definition

- Our Security and Fraud subject matter experts can help you to
  - Define, document, validate and implement Risk Assessment Methodologies
  - Procedures (i.e. for the annual risk assessment of customers and business partners) as well as
  - Risk scenarios.
- All three elements form part of the ECB requirements on your Risk Management function and are at the core of the new minimum expectations

Operating Model Change

- We can support you on all or selected areas of the operating model design and implementation across the payment service value chain and in recognition of the impact of any change on your customers and colleagues of your business areas.
- With deep subject matter expertise around Customer Due Diligence, Risk Engines, Behavioral Analytics, Transaction Monitoring and Fraud Detection as well as Operational Model Definition and Implementation we can help to roll-out your change program in time for 1 FEB 2015

- Last but not least, we can support you in the dialogue with the regulators. Our strong experience with the local and supra-national regulators in Europe, the US and elsewhere is a key benefit we can bring into the preparation of your regulatory meetings, correspondence and actual deliverables

We understand the challenges you face

Customer Service

- Security and fraud measures are not always understood by customers as something they benefit from, therefore effective communication of the reasons for certain controls is crucial in getting the customer buy-in

Regulatory Changes

- Regulation related to internet payment security is constantly evolving – it is a 'moving target' and getting clarity on matters related to fast moving new methodologies and technologies is tough. In order to become compliant providers must implement costly current and future regulatory changes concurrently with other critical business changes

Efficiency and Cost

- The cost of implementing and running effective security & fraud management needs to be carefully balanced against the impact it has on customer service, as i.e. stringent fraud detection measures may lead to a rise in customer complaints

Enabling Technology

- Effective security & fraud management requires the deployment of sophisticated and up-to-date technology. This is costly, and the impact on customer experience needs to be understood

Our insight into the market

Ernst & Young has a strong track record with leading global and local payment service providers and is ideally positioned to support you on the implementation of both, robust policies and a supporting operating model.

We have a deep understanding of the complex range of factors which will inform decisions on how to define a risk based approach and – more importantly – how to operationalise it. We are ideally positioned to support all scales of payment service organizations as we offer

- A multi-disciplinary, multi-lingual team based in Germany, UK, US, France, Netherlands and the Nordics that can work collaboratively with your team wherever needed.
- Access to deep expertise on the local payments market, both digital and traditional.
- Perspectives on digital payment drivers and developments in digital commerce to 2016.
- A track record of delivering successful payment operating model change and cross-border implementations as an independent advisor which gives us an initial view as to how your integration might look.
- A proven and flexible approach to delivery of your implementation.
- A tailored commercial proposal with different implementation options.

Our significant knowledge around the payment service industry and its regulators will be a decisive factor in driving progress and minimizing delivery risk towards the formal deadline 1 FEB 2015.

Our team includes payment experts who have done this before and can mobilize immediately. We are keen to continue the journey towards a more sophisticated market practice with you and hope that our ideas demonstrate our commitment to continuing our partnership with the payment service industry.

Contact us

Germany

Christopher Schmitz
Partner
+49 6196 996 13545
christopher.schmitz@de.ey.com

Dominik A. Käfer
Senior Manager
+49 6196 996 15817
dominik.kaefer@de.ey.com

United Kingdom

Hamish Thomas
Director
+44 7967 176 593
hthomas@uk.ey.com

France

Pierre Pilorge
Partner
+33 1 46 93 59 79
pierre.pilorge@fr.ey.com

Netherlands

Steven Hartjes
Partner
+31 88 40 71541
steven.hartjes@nl.ey.com

Sweden

Karin Sancho
Partner
+46 8 52059767
karin.sancho@se.ey.com

Ernst & Young
Assurance | Tax | Transactions | Advisory

About the global Ernst & Young organization
The global Ernst & Young organization is a leader in assurance, tax, transaction and advisory services. It makes a difference by helping its people, its clients and its wider communities achieve their potential. Worldwide, 167,000 people are united by shared values and an unwavering commitment to quality.

The global Ernst & Young organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity's acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information, please visit www.de.ey.com

In Germany, Ernst & Young comprises some 7,400 people at 22 locations. In this publication, "Ernst & Young" and "we" refer to all German member firms of Ernst & Young Global Limited.