# Securing Critical Infrastructures In The Financial Sector

## Regulation in the Financial Sector and its Impact on Financial Technologies

# Objectives


*Regulations relevant to the financial sector*

*Goal*

- Learn about most widely used regulations in the financial sector
- Understand the objectives of each of the regulations
- Explore the scope of regulations
- Realize its impact for financial technologies

# Introduction

- Different requirements for financial security
- Plethora of different regulations, standards and directives
- National, regional or global level
- Frame the way in which financial infrastructures acquire, handle, store, communicate and process information
- Frame the way in which financial infrastructures acquire, handle, store, communicate and process information
- Fulfil limitations, extend or complement existing regulations or standards

❖Standardization landscape for the financial sector is evolving at a very fast pace


# *Regulations relevant to the financial sector*

# List of regulations to be addressed

- Markets in Financial Instruments Directive II – MiFiD II
- Payments Services Directive (PSD 2) - Directive 2015/2366
  - PSD2 - Regulatory Technical Standards (RTS)
- PCI DSS and PCI 3DS
- National regulatory bodies
  - German supervisor authority (BaFIN)
- European Banking Authority III
- Regulation for insurance security
- European Central Bank (ECB) cyber incident reporting regime

# Markets in Financial Instruments Directive II – MiFiD II

| *Characteristics* | *Details* |
|---|---|
| ⌘ Content | ■ Markets in Financial Instruments Directive (“MiFID”)<br>■ Regulation on Markets in Financial Instruments and Amending Regulation (“MiFIR”) |
| ⌘ Application area | ■ Europe-wide |
| ⌘ Objective | ■ Regulating the operation of financial markets in the European Union |
| ⌘ Focus | ■ Framework of trading venues/structures in which financial instruments are traded<br>■ Regulating the operation of trading venues/structures, looking to processes, systems and governance measures adopted by market participants and to their future supervision. |

# Markets in Financial Instruments Directive II – MiFiD II

| *Characteristics* | *Details* |
|---|---|
| ⌘ Scope | ■ Safer, sounder, more transparent and more responsible financial system<br>■ Enhances algorithmic trading activities: it introduces trading controls for algorithmic trading activities, leads to much increased speed of trading |
| ⌘ Impact on financial sector | ■ Investment firms enforced to have in place systems and risk controls such that they could effectively prevent trading that may contribute to a disorderly market or involve market abuse |
| ⌘ Impact on financial technologies | ■ Enforces brokers to increase the information reported → Traders gain extended transparency<br>■ Mandates the testing of algorithms used for algorithmic trading and addition of enhanced tags to precisely identify the origins of an order |

# Payments Services Directive (PSD 2) - Directive 2015/2366

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Content | ■ Revised Payment Services Directive (PSD2) |
| ⌘ Application area | ■ Europe-wide? |
| ⌘ Objective | ■ Enhance innovation potential, competition and efficiency in electronic markets |
| ⌘ Focus | ■ Offer consumers more and better choice in the EU retail payment market<br>■ Introduce higher security standards for online payments |

# Payments Services Directive (PSD 2) - Directive 2015/2366

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Scope | ■ Changes with respect to the range of transactions, the scope of stakeholders, liability and information and security assessment<br>■ Extend the EU's regulatory framework on transactions<br>■ Enhance the Payment Service Provider (PSP) with an additional category:<br>  ■ Third-Party Service Providers (TPSPs)<br>  ■ Account Information Service Providers (AISPs)<br>  ■ Payment Information Service Providers (PISPs) |
| ⌘ Impact on financial sector | ■ Financial institutions to fulfil account information and payment initiation requests by providing TPSPs with the necessary information via Application Programming Interfaces (APIs)—given that they will be authorised by the payer |

# Payments Services Directive (PSD 2) - Directive 2015/2366

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Impact on financial sector (cont.) | ▪ Payers to gain additional protection for the case of any incorrectly executed payments<br>  ▪ Payments will need to be processed through “strong customer authentication”<br>  ▪ Unlikely for information related to the payer to be retained for any other purposes than completing the payment |
| ⌘ Impact on financial technologies | ▪ Financial institutions to ensure their compliance with additional information and technology requirements<br>▪ Set up APIs such that it will encapsulate specific monetised services, existing margins, and simplified and optimised infrastructure<br>▪ Strong customer authentication |

# Payments Services Directive (PSD 2) - Directive 2015/2366

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Impact on financial technologies (cont.) | ■ Ensure compliance with additional information and technology requirements<br>■ Set up APIs such that it will encapsulate specific monetised services, existing margins, and simplified and optimised infrastructure<br>■ Strong customer authentication<br><br>■ Third Party Service Providers (TPSPs) perspective : Set up risk and control frameworks, comply with all relevant reporting obligations, and perform AML and KYC controls |

# PSD2 - Regulatory Technical Standards (RTS)

| *Characteristics* | *Details* |
|---|---|
| ⌘ Content | ■ Regulatory technical standards (RTS) on the basis of the draft submitted by the European Banking Authority (EBA)<br>■ RTS for strong customer authentication (SCA) and secure open standards of communication (CSC) are the basis for the implementation of PSD2 |
| ⌘ Objective | ■ Safer and more innovative electronic payments |
| ⌘ Focus | ■ RTS formulate specific security measures to ensure the effective and secure communication between relevant actors |

# PSD2 - Regulatory Technical Standards (RTS)

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ SCA | ▪ Requires that the customer's identity is verified using at least two mechanisms of the:<br>  ▪ knowledge (i.e., something that only the user knows e.g., Password)<br>  ▪ possession (i.e. something only the user possesses, e.g., a card, mobile phone)<br>  ▪ inheritance (i.e. something the user is, e.g., biometric) |
| ⌘ CSC | ▪ Regulates the way the customer's account is shared between the ASPSP and the AISP or PISP<br>▪ Secure communication channel will be established to provide access to the payment account<br>▪ RTS requires customers to provide their explicit consent to the AISP or PISP to share their payment account details or initiate a payment transaction |

# PSD2 - Regulatory Technical Standards (RTS)

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Impact on financial technologies | ■ Payment services providers (PSPs) need to ensure that their technology and infrastructure provides customers with the ability to identify themselves using more than one authentication mechanism<br><br>■ To achieving SCC:<br>■ Option #1: to create an API that will provide identical level of availability and performance as the customer's online interface and it will also enable the provider to also offer a payment initiation of account information services without any obstacle.<br>■ Option #2: Offer an adaptation of the customer's online banking interface. Adaptation of the customer's payment account, accessed using personalized security credentials by the TPP such that it can be adjusted to desired interface. |

# PCI DSS and PCI 3DS

| *Characteristics* | *Details* |
|---|---|
| ⌘ Content | ■ Payment Card Industry Data Security Standard (PCI DSS) issued by the Payment Card Industry Security Standards Council<br>■ Three-Domain Secure (3DS) is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making e-commerce purchases |
| ⌘ Application area | ■ Worldwide |
| ⌘ Objective | ■ To secure card payments |
| ⌘ Focus | ■ Ensure that 'cardholder data' as the full Primary Account Number (PAN) and other card information (e.g. Cardholder name, expiration date, CVCs etc.) are protected<br>■ Prevent unauthorized transactions where the "Card is not Presented" and protect the merchant from fraud |

# PCI DSS and PCI 3DS

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Scope | ■ PCI DSS<br>■ very specific to the payment card sector<br>■ relevant to the payment functions of business systems<br><br>■ Compliance of PCI DSS is imposed by Credit card processors to card issuers and merchant banks<br><br>■ Introduces requirements, including:<br>■ establishment of an effective operational and security risk management framework<br>■ processes that detect, prevent and monitor potential security breaches and threats<br>■ risk assessment procedures<br>■ regular testing<br>■ processes that raise awareness to Payment Service Users on security risks and risk-mitigating actions |

# PCI DSS and PCI 3DS

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Impact on financial technologies | ■ Protection expected from cyber-physical threats<br>■ Requires the establishment that any physical access to data or systems that house cardholder data are protected |

# National regulatory bodies – German supervisor authority (BaFIN)

| | |
|---|---|
| ⌘ Content | ▪ BaFin is the (German) acronym for the Federal Financial Supervisory Authority in Germany |
| ⌘ Geographical area | ▪ Germany |
| ⌘ Objective | ▪ Introduces supervisory requirements for IT in financial institutions (BAIT) |
| ⌘ Focus | ▪ BAIT :<br>  ▪ encapsulates requirements lead to the secure design of IT systems and of the associated processes and IT governance<br>  ▪ contains interpretation of the legal regulations according to German Banking Act and the Minimum Requirements for Risk Management :<br>  ▪ appropriate technical and organisational equipment of IT systems for information security and adequate contingency planning |

# European Banking Authority III

| *Characteristics* | *Details* |
|---|---|
| ⌘ About | ▪ Independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector |
| ⌘ Geographical area | ▪ Europe-wide<br>▪ Regulation (EU) No 1093/2010 establishing the EBA requires that competent authorities and financial institutions make every effort to comply with the EBA guidelines and recommendations (Article 16) |
| ⌘ Objective | ▪ To maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector |
| ⌘ Focus | ▪ Efficient and effective supervisory practices across the EU and ensure uniform application of Union law<br>▪ Regulatory guidelines and recommendations |

# European Banking Authority III

| *Characteristics* | *Details* |
| --- | --- |
| ⌘ Scope | ■ Article 9(2) of the EBA's Founding Regulation mandates the Authority to monitor new and existing financial activities<br>■ Obligation extends to all areas of the EBA's competence, including the field of activities of credit institutions, financial conglomerates, investment firms, payment institutions, and electronic money institutions |