Adapting to a New Regulatory Environment in Europe

Tim Roberts

London

24 May 2017
Near term drivers of regulatory change

- **Payment Services Directive 2 (PSD2)** – driving banks towards a new era of open banking and payments.
- **General Data Protection Regulation** – requiring a step change for all firms that hold data.
- **MiFiD 2 and MAD/MAR** – requiring post-trade transparency, best-ex tools, and major investment in technology for trade surveillance to detect behaviors that impact market integrity.
- **Cyber Security and Resilience** – new regulations and heightened expectations from regulators around the world concerning security and resilience.

Longer term priorities

- **Risk culture and conduct.** On the heels of the Wells Fargo sales practices enforcements, we see strong knock-on effects for the entire industry. Leading firms are creating conduct and culture metrics to measure and monitor behaviours.
- **Technology enablement for compliance and risk.** It is rapidly becoming the case that risk and compliance functions cannot rely on human capabilities alone to be effective – there is a need to augment these processes with advanced analytics and machine learning.
Key Components of PSD2 Compliance

PSD2 was formally adopted in November 2015 and will be implemented at a national level by 13 January 2018.

The aim is to enhance competition within EU payment services by opening up access to banks’ payment services platforms and by harmonising legislation across the EU.

A major impact for Account Servicing Payment Service Providers (ASPSPs), the banks or other institutions providing and maintaining payment accounts, is that they will be obliged to allow access to account information for all online accounts to Account Information Service Providers (AISP), and to allow the ability to initiate payments on an account holder’s behalf by Payment Initiation Service Providers (PISP).

<table>
<thead>
<tr>
<th>Obligation type</th>
<th>Entity type</th>
<th>ASPSP</th>
<th>Third party payment providers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ASPSP</td>
<td>PISP</td>
</tr>
<tr>
<td>Technical</td>
<td>Access to accounts</td>
<td>Payment initiation</td>
<td>Strong authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Account information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Confirmation of funds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Interoperability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strong authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of TPPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fraud monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td>Access to accounts</td>
<td>Interoperability</td>
<td>Identificatio...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strong authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of TPPs</td>
</tr>
<tr>
<td></td>
<td>XS2A SCA Regulatory Technical Standard</td>
<td>Fraud monitoring</td>
<td>Liability insurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of TPPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fraud monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security measures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identification of TPPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Financial</td>
<td>Liability insurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Capital requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Incident management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Complaints management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Record consent</td>
</tr>
<tr>
<td>Processes</td>
<td></td>
<td>Incident management</td>
<td>Incident management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Complaints management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Record consent</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Incident management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Complaints management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Record consent</td>
</tr>
</tbody>
</table>
Benchmarking Banks’ Preparations for PSD2

Risk of significant issues on implementation

Low

High

Parallell发展 of legacy and new platform

Legacy platform

New platform

We would observe the following points from this overview of current status among the firms interviewed:

• Only 3 out of 8 would currently stand out as low risk

• The best positioned firms are either in markets with more advanced digital banking or are fintechs themselves

• The higher risk firms either started later, or are building on a legacy platform
Overview

• The General Data Protection Regulation (GDPR) is the first comprehensive overhaul of European Union data protection rules in 20 years - it repeals and replaces Directive 95/46/EC and will be directly applicable in all EU Member States

• The European Commission first published a proposal for the GDPR in January 2012. After over four years of negotiations, the GDPR will enter into force on 25 May 2016 and will go live on 25 May 2018

• The GDPR will apply to data controllers and processors, regardless of their location, that process the personal data of people in the EU in the context of offering goods or services in the EU, or monitoring their behaviour

• The GDPR will provide
  o enhanced rights for data subjects,
  o additional obligations for data controllers and processors, and
  o a new cross-border regulatory regime with stronger enforcement powers

Administrative fines

• Up to the greater of €20 million, or 4% of worldwide annual turnover (revenue) for infringements regarding the principles for processing, data subject rights, transfers, or noncompliance with an order; €10 million or 2% for infringements of obligations of controllers and processors

One-stop shop

• Lead authority model introduced but ‘local’ cases can dealt with by local supervisory authorities

• If a concerned supervisory authority objects to a lead authority’s draft decision, the case shall be referred to the European Data Protection Board for a binding decision
Regulators, law enforcement and investors are focused on market abuse as evidenced by large fines and legal suits. Promontory has conducted a rigorous review of surveillance regimes in a number of global firms. IBM/Promontory are developing Watson to surveil e-comms and monitoring systems to enhance efficiencies and effectiveness.

**Key areas**
- Map all relevant regulation to activities
- Perform Risk Assessment
  - Granular evaluation of the inherent risks in each business activity
  - A qualitative and quantitative assessment of control effectiveness
  - Recommend control enhancements
  - Deliver an action plan to implement practical solutions to address identified gaps

**Example of heat map of market abuse risk**

**Review of the Trade Surveillance Organization**

**Key areas**
- Analyze the adequacy of the organization, including the allocation of roles and responsibilities in first and second line of defense
- Verify the existence of a set of clearly formalized policies and procedures for escalation between first and second line
- Check procedures for alerts and investigations

**Assessing Specific Control Tools and Review Rule and Process Optimization**

**Key areas**
- Assess the implementation of specific control processes, tools and methodologies
- Evaluate accuracy, robustness, and completeness of processes used by the Bank for monitoring its transactions
- Check the methods used to review and report on the performance and effectiveness of the rules and scenarios to optimize rule selection and calibration
- Assess the monitoring and measurement compliance activities through key performance indicators (KPI)
- Evaluate the accuracy and timeliness of the reporting system (dashboard) to inform management about performance
From our experience with wholesale firms’ MiFID II programs, to the right are the key implications of MiFID II that are impacting the operating models, and where more substantial attention is required. 

*(red = high impact, orange = mid impact, grey = low impact)*

<table>
<thead>
<tr>
<th>Markets</th>
<th>Client Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-trading transparency</td>
<td>Suitability / Appropriateness</td>
</tr>
<tr>
<td>Transaction Reporting</td>
<td>Recording of conversation</td>
</tr>
<tr>
<td>Algo Trading</td>
<td>Information on Costs / Reporting</td>
</tr>
<tr>
<td>Underwriting/Placement</td>
<td>Inducements</td>
</tr>
<tr>
<td>Trading obligations</td>
<td>Investment Research</td>
</tr>
<tr>
<td>Product Governance</td>
<td>Record Keeping</td>
</tr>
<tr>
<td>Post-Trade transparency</td>
<td>Safeguarding of client asset</td>
</tr>
<tr>
<td>Best Execution</td>
<td></td>
</tr>
</tbody>
</table>

**Key challenges we have observed**

**MiFID II programme**
- Is decision-making taking place effectively, particularly for cross-regional businesses?
- Local change requirements vs decision making and budgets controlled overseas
- Dealing with uncertainty
- Sufficiency of resource to drive size of program
- Mapping of rules to the implementation plan and audit trail of compliance

**Strategic matters:**
- Connectivity between dealers and future trading platforms
- Register as Systematic Internalizer?
- Identifying strategic opportunities and threats
- Advisory and execution model
- Front to back target operating model

**Technology**
- Re-build new infrastructure to fix historical issues?
- Invest in global data warehousing?
- Strategic vs tactical solutions to comply (cost control initiatives)
- External system vs internally developed system
- Dealing with uncertainty of regulatory requirements
Key Regulatory Concerns About Financial Institutions’ Technology

**Resilience**

- Financial institutions have always been vulnerable to failures of resilience
- However, the acceleration towards use of cloud services by banks and customer demand for mobile and digital banking escalates dramatically both the potential consumer detriment and the systemic impact of failures

**Security**

- Regulators are increasingly focusing on the risks from outsourcing, adoption of cloud, digital banking models and a rapidly developing attacker industry
- Regulators are also seeking greater rigour around incident management and reporting, as well as prevention

**Privacy**

- Around the world, consumers are becoming more concerned about their personal data and how it is used
- Governments in multiple jurisdictions are stepping up oversight of this set of risks; the EU’s GDPR raises the stakes significantly

**Data quality**

- Regulators are concerned about the quality and reliability of data being used by firms for key analytic functions – risk quantification, capital calculation – and screening processes such as AML and market abuse
- Regulators are also concerned about firms’ ability to deliver reliable regulatory reporting and respond accurately to investigations
Key Business Concerns about Technology and Risk

1. Target Operating Model
   - What are the right operating model, organisation structure, and roles & responsibilities to deliver a full cyber risk management framework across the enterprise?
   - What new skills are required to provide independent challenge across the three lines of defence?
   - What resourcing levels are appropriate given the threat environment?

2. Metrics, Monitoring and Reporting
   - How should the firm track its risk profile and control effectiveness for cyber security?
   - How do the top level KRI/KPIs cascade down to a full dashboard for the management of cyber risk?
   - How do firms ensure incidents are detected and reported within regulatory timeframes?

3. Board Engagement
   - How should the Board engage with the management of cyber risk?
   - What do they need to be effective in that role – training, information, reporting, engagement?

4. Culture and Behaviours
   - What is the human component of the control framework, and how effective is it?
   - How should staff be educated, engaged, managed and motivated to contribute to a secure environment?

5. Third Party Risk Management
   - How does the firm manage its wider cyber risk profile across suppliers, intermediaries, customers – including managing concentration risk among key suppliers?
   - How does the firm outsource to the cloud and still comply with regulatory requirements such as GDPR and resilience?

6. Incident Management
   - How ready are the Board and the executive team to handle a cyber incident?
   - Are appropriate plans in place? Have they been rehearsed?
   - Does the firm have appropriate incident classification and escalation/regulatory reporting rules?
A Constant Challenge – Dealing with Events

WannaCry ransomware attack

No warning of major attacks

Increasing danger of sophisticated government-designed weapons in criminal hands

Protection requires the basics to be done consistently
– Patching
– Training
– Incident plan preparation
– Incident plan rehearsal

This reinforces the need to embed cyber security into everyday governance and risk management
Cyber Risk Management and Compliance

Strategy
Setting the overall strategic approach to assessing and managing risk, and the risk appetite that fits with business goals and the firm’s environment
Outlining the budget, roadmap and implementation approach

Governance
Definition of the organizational roles and responsibilities, policy framework and arrangements for oversight of the risk profile and party risk management framework

Controls
The control environment which delivers the chosen risk appetite and enforces the policy framework

Monitoring, Measuring & Management Information
Monitoring of threats, incidents and the performance of controls
Track the performance of risk management against risk appetite, using quantitative metrics where possible

Feedback loop – from front line controls to overall strategy

External Communication & Stakeholder Management
Managing external reporting requirements and requests, and engagement with external stakeholders such as regulators
Regulatory Focus Intensifying on Culture and Conduct

• The U.S. Federal Reserve is clearly still minded to bring new perspectives on culture and the tools for its development and management, including compensation. However, while academic attention is most likely to deliver longer term insights – it leaves open the need for practical tools for use today.

• The FCA’s current views emphasise persistent senior management focus:
  o The FCA is not seeking to be prescriptive – **firms must define their own culture** based on their business, their operating model and style of doing business.
  o It is recognized that **culture and mindsets are slow to change** and build up over years. They believe there are significant pitfalls to firms that are overly target-focused – this can lead to abuse of the target metrics rather than focus on the underlying outcomes.
  o What they want to see is an **enduring, dynamic focus** from senior management on both the inputs to mindsets and behaviors within the business and the **outcomes** for customers and markets.
  o They believe there is no **‘silver-bullet’ set of metrics** that will perfectly illustrate culture; rather, it requires boards and senior management to look across both inputs and outcomes, over time, to check that the inputs are changing behavior for the better, and that the firm is delivering good outcomes.
Measuring and Managing Culture – Four Repeatable Steps

1. Define the behaviours you wish to see in the organisation in order to stay within risk appetite, in line with the business mix, geographical footprint and strategic objectives.

2. Communicate and embed the behaviours in the day to day practices visible across the organisation.

3. Reinforce the behaviours with formal tools like training, evaluation, compensation.

4. Measure and actively monitor the extent to which the desired behaviours have genuinely become ‘how we work around here’, and the results, through a flexible but rigorous set of metrics.
Culture Management Requires Metrics and Indicators

Promontory Culture Metric Library
Categories of metrics/indicators

1. Governance and leadership
2. Talent management/incentives
3. Risk and compliance practices
4. Business Execution

Examples of Culture and Conduct Indicators

Firms must develop indicators for monitoring culture that are tailored to their specific characteristics, including information systems, approach to performance evaluation, and business mix, among many other things. While the indicators at each institution will vary, the examples below are representative of the types of metrics that financial institutions may already have, or that can be developed through surveys or other means. The indicators may be collected at the enterprise level, business-unit level, or both.

**Risk and Compliance Management Metrics**
- Number of risk policy breaches
- Number and frequency of non-ensured losses
- Number of requests for exceptions to policy
- Number of instances where required policy approval was not obtained
- Trade surveillance
- Number of trade-surveillance alerts triggered (trading before major news, unusual activity)
- Number of alerts triggered through client monitoring processes monitoring
- Whistleblower reports/investigations
- Number of whistleblower investigations raised through firm’s anonymous portal
- Number of whistleblower investigations resulting in disciplinary action

**Human Resources Metrics**
- Employee discipline:
  - Percentage of employees who had low conduct ratings in performance assessments and received high bonuses or rewards
  - Percentage of employees who have significant past disciplinary records or a number of settled sales-practice complaints or arbitrations
- Training:
  - Percentage of employees who completed mandatory training (by level and function)
  - Percentage of employees required to take mandatory training
- Conduct:
  - Number of conduct violations
  - Number and nature of ethics/compliance conduct violations

**Business-line Indicators**
- Number of product lines with year-over-year revenue growth of > 25% with breakdown by business unit or geography
- Number and severity of line-of-business control breaks identified by line of business as those identified by compliance

**Results of Internal Audit Reviews**
- Number/percentage of repeat high-risk issues identified during audits
- Percentage of past-year audit items and matters for being past due

**Results of Supervisory Reviews**
- Number of supervisory actions such as MRA (matters requiring attention) and MRM (matters requiring immediate attention)
- Supervisory ratings on risk management, compliance, reputation risk

**Information Drawn from Employee Surveys**
- Employees’ knowledge:
  - Percentage of employees who are aware of the firm’s escalation and/or whistleblower policies
  - Percentage of employees who understand all requirements and expectations related to their role in managing risk
- Employee beliefs:
  - Percentage of employees who believe that management exhibits integrity
  - Number of employees who believe their direct supervisor is receptive to employees “speaking up”

**Reputation Indicators**
- Negative comments about the firm on social media or other public-opinion sites
- Violations of consumer law
- Number and nature of customer complaints
Scope for Technology to Augment Human Insight

Human surveillance is, by definition, limited – it can only see what a person can see without disturbing the subject. If culture is defined as ‘how people behave when no one is looking’ then human surveillance is by definition limited, even useless. However human skills, experience, insight and foresight are essential to ensure surveillance is ‘street smart’ and can be forward looking.

Technology allows subtle surveillance techniques to go where a senior manager cannot, and to leverage insight into rigorous screening – the ideal surveillance technology is cognitive, blending human insight with technological rigour.

- **Technological screening and analytics**: Same input will generate same outputs. Consistent interpretation of results. Repeatable, not dependent on human operator.
- **Human judgement and adaptation**: Technology augments human expertise and imagination. Optimises against efficiency and use of expertise when it is valuable.
- **Ability to use experience and spot links between unconnected events**: But – labour intensive and processing manual, so prone to errors.
Example: Moving Towards Integrated, Cognitive Surveillance
Thank you