EU and Eurozone growth and integration challenges: the moment of truth?

Jacques de Larosière
President, EUROFI

Pierre Gramegna
Minister of Finance, Luxembourg
About EUROFI
The European Think Tank dedicated to Financial Services

A not-for-profit organization chaired by Jacques de Larosière
A platform for exchanges between the financial services industry and the public authorities addressing issues related to the evolution of financial regulation and supervision and the economic and monetary context impacting the EU financial sector

MAIN ACTIVITIES

The main objectives of Eurofi are to help industry and public decision-makers reach a common understanding of possible evolutions required in the regulation and supervision of financial services and to open the way to legislative or industry-driven solutions that may enhance the safety and effectiveness of the EU financial sector and its contribution to economic growth.

Eurofi acts in a general interest perspective, facilitating exchanges of views between diverse financial industry players and the public authorities. These exchanges are prepared by objective fact finding and issue analyses.

Eurofi has two main types of activities conducted by Didier Cahen, Secretary General of Eurofi, Jean-Marie Andrès and Marc Truchet, Senior Fellows:

- **Events and meetings:**
  - Eurofi organizes annually two major international events (the High Level Seminar in March / April and the Financial Forum in September) gathering industry leaders and EU and non-EU public decision makers for discussions on the major on-going regulatory projects in the financial area and the role of the financial sector in fostering growth as well as informal networking.
  - These events are regularly organised in association with the EU Presidencies in parallel with informal ECOFIN councils and in some cases with the G20 Presidencies. They are organised with the support of Virginie Denis and her team.
  - Additional workshops involving the members of Eurofi are set up to exchange views on regulatory issues. Bilateral meetings are also regularly organised with representatives of the public authorities and other stakeholders (e.g. end-users, experts) to fine-tune assessments and proposals.

- **Research and documentation:**
  - Assessments and proposals taking into account economic, risk and end-user impacts are prepared with the support of cross-sectoral working groups comprising members of Eurofi.
  - Topics addressed include prospective and on-going regulatory proposals at the EU and global levels, industry trends as well as the impacts for the financial sector of the economic challenges the EU is facing.

MAIN TOPICS CURRENTLY ADDRESSED

- **Measures and instruments needed to ensure an appropriate financing of the EU economy:** assessment of the economic challenges to be addressed in the EU impacting the financial sector and of the impact of on-going monetary actions, measures to support bank financing (securitisation) and further diversify the financing of SMEs and infrastructure projects, proposals for developing a long term investment perspective, measures to stimulate EU bond and equity markets...

- **Prospects of further EU integration:** implementation of the Banking Union, priorities for implementing a Capital Markets Union, possible evolution towards a fiscal union and supervisory authorities (ESRB, ESAs).

- **Optimizing the EU financial services internal market:** conditions for enabling a sustainable SEPA business case, review of the IORP directive, regulation of CRAs, prospects of further banking integration...

- **Evolutions of the prudential and regulatory framework of banks and insurance companies:** fine-tuning and implementation of banking and insurance prudential frameworks (liquidity provisions, RWA evaluations, Solvency II), recovery and resolution of banks and non-banks, digital financial services...

- **Capital markets and investment products regulations:** Capital Markets Union, regulation of securities, derivatives and commodities markets and infrastructures, recovery and resolution of CCPs, cybersecurity, SFT and collateral requirements, asset management regulations, investor protection regulation (PRIIPs, MiFID, IMD...), regulation of shadow banking

- **Financial regulation at the global level:** feasibility of bank crisis management at the global level, coordination of capital markets regulations at the global level, systemicity of non-banks non-insurers...

EUROFI MEMBERS

The membership of Eurofi comprises many leading global and European financial institutions from different sectors of the industry (banking, insurance, market infrastructures, asset management, credit rating agencies...).
The Eurofi Financial Forum 2015

Organised in association with the Luxembourg Presidency of the EU Council

9, 10 & 11 SEPTEMBER // LUXEMBOURG

EU AND EUROZONE GROWTH AND INTEGRATION CHALLENGES: THE MOMENT OF TRUTH?
## EU AND EUROZONE GROWTH AND INTEGRATION CHALLENGES: THE MOMENT OF TRUTH?

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDITORIAL</td>
<td>5</td>
</tr>
<tr>
<td>VIEWS OF THE LUXEMBOURG EU COUNCIL PRESIDENCY</td>
<td>9</td>
</tr>
<tr>
<td>GROWTH AND INTEGRATION CHALLENGES IN THE EU</td>
<td>14</td>
</tr>
<tr>
<td>EMERGING TRENDS IN THE FINANCIAL SERVICES SECTOR</td>
<td>38</td>
</tr>
<tr>
<td>IMPLEMENTING THE CMU &amp; ASSET MANAGEMENT FUTURE PROSPECTS</td>
<td>62</td>
</tr>
<tr>
<td>ENSURING THE RESILIENCE OF THE EU FINANCIAL SECTOR</td>
<td>102</td>
</tr>
<tr>
<td>GLOBAL COORDINATION OF REGULATION</td>
<td>126</td>
</tr>
</tbody>
</table>
The cyber-risk facing the financial sector is unprecedented, potentially systemic and global. Cyber-attacks targeting financial actors, services and infrastructure can not only result in high economic cost but also undermine the integrity of our financial system, through disruption and sabotage.

IOSCO has taken notice of this reality and over the last three years, we have been working to understand the nature of the threat and improve the cyber-resilience of financial markets through research, policy work, international cooperation and collaboration with other organizations such as the Committee on Payments and Market Infrastructures.

There are a number of unique and complex challenges that must be overcome. Most of these challenges can be characterised as pertaining to asymmetric capabilities between perpetrators and their targets; and the global nature of the threat.

Since the cyber-risk is a global issue no one firm or jurisdiction can deal with it in isolation. Cyber-attackers themselves are not constrained by national borders or regulatory jurisdiction. However, actors aiming to protect the financial sector from these attacks must operate within these parameters. While cyber-attackers have access to sophisticated cross-border, collaboration and information sharing networks, housed on the dark web; similar networks available to regulators and authorities are generally national in nature only. Cross-border information sharing platforms are almost non-existent or at an infant stage of development. On top of this, cyber-attackers have an offensive advantage. Many of the current approaches to improving the cyber resilience of the financial system are defensive while offensive tools used by cyber-attackers are rapidly evolving. The cost of putting in place sophisticated and adaptable defensive security measures to deal with an evolving threat far surpasses the cost of launching an attack.

To overcome these challenges and level the playing field, it is imperative that adaptable, holistic and forward-looking cyber-resilience approaches be encouraged alongside strong international and cross-sectoral cooperation and information sharing.

Cyber risks in exchanges and clearinghouses: a regulator’s approach

Jeffrey M. Bandman - Special Counsel to the Chairman, Office of the Chairman & Acting Director, Office of International Affairs, U.S. Commodity Futures Trading Commission (CFTC)

Cybersecurity is perhaps the single most important threat to market integrity and financial stability. Cyberattacks threaten privacy, information security, and business continuity, all vital elements of a well-working market.

The CFTC, as a regulator, can set standards and perform examinations. But ultimately the private sector must take responsibility for the comprehensive work required to safeguard critical infrastructure at each firm. While we do not mandate the specific mechanisms that an exchange or clearinghouse should use in the cyber area, through our examinations of clearinghouses and exchanges we seek to ensure that critical financial infrastructure subject to CFTC
oversight has in place appropriate business continuity and disaster recovery plans to address these risks.

With respect to cybersecurity in particular, we require clearinghouses and exchanges to maintain system safeguards and a risk management program, to notify the CFTC promptly of incidents, and to have recovery procedures in place. They must also keep personnel dispersed geographically to aid recovery efforts following a disruption.

We conduct system safeguards examinations, using industry best practices, to determine compliance with these requirements, and we monitor remediation efforts if issues are identified during the examination process. We are making sure the private companies that run major exchanges and clearinghouses are doing adequate testing themselves of their cyber protections, such as control testing, penetration testing, and vulnerability testing. Testing works best when testing fails, meaning when it is pushed to the point that you truly identify weaknesses or a penetration occurs so that you can remedy the problem.

We also look at whether the institution is following best practices: is the board of directors focused on the issue; is adequate expertise in place at a senior level; is there a culture in which cybersecurity is given a priority; has the entity not only adopted good policies on cybersecurity, but are those policies being observed and enforced?

We work closely with other regulators on these concerns, in the US and abroad. To help ensure coordination and better information sharing between government and private sector we work with the US Financial Services Sector Coordinating Council. We also encourage our registrants to participate in the cybersecurity information sharing conducted across the financial sector, including anonymized information sharing after a firm has experienced a cyber attack. Finally, we expect to propose a new rule on this subject later this year, which would set forth requirements on testing to insure best practices are being followed.