afme/ Finance for Europe

Association for Financial Markets in Europe

Cyber Security

The increasing global risk for firms

21 September 2017

Andrew Harvey, Managing Director, GFXD Europe, GFMA
David Ostojitsch, Director, Technology and Operations, AFME
Emmanuel Le Marois, Manager, Technology and Operations, AFME
Dave Evans, Director, Cyber Resilience, UBS

afme/ Finance for Europe

Association for Financial Markets in Europe

Member Briefing Call Introduction

Andrew Harvey, Managing Director, GFXD Europe, GFMA

afme/ Finance for Europe

Association for Financial Markets in Europe

AFME Technology and Operations Division

David Ostojitsch, Director, Technology and Operations, AFME

Key Tech and Ops Market Drivers Today

Increasing cyber risks and events

Policy and supervisors

There is a growing shift to a technology and cyber-centric policy agenda with increased supervisory access and oversight

Fintech and competition

New market participants are driving change to traditional models and competitors are rethinking financial services (Amazon lending, P2P and crowdsourcing).

Emerging technologies

There is an increasing focus on blockchain, artificial intelligence, machine-to-machine interactions, and tokenisation (cryptocurrency).

Operating environment

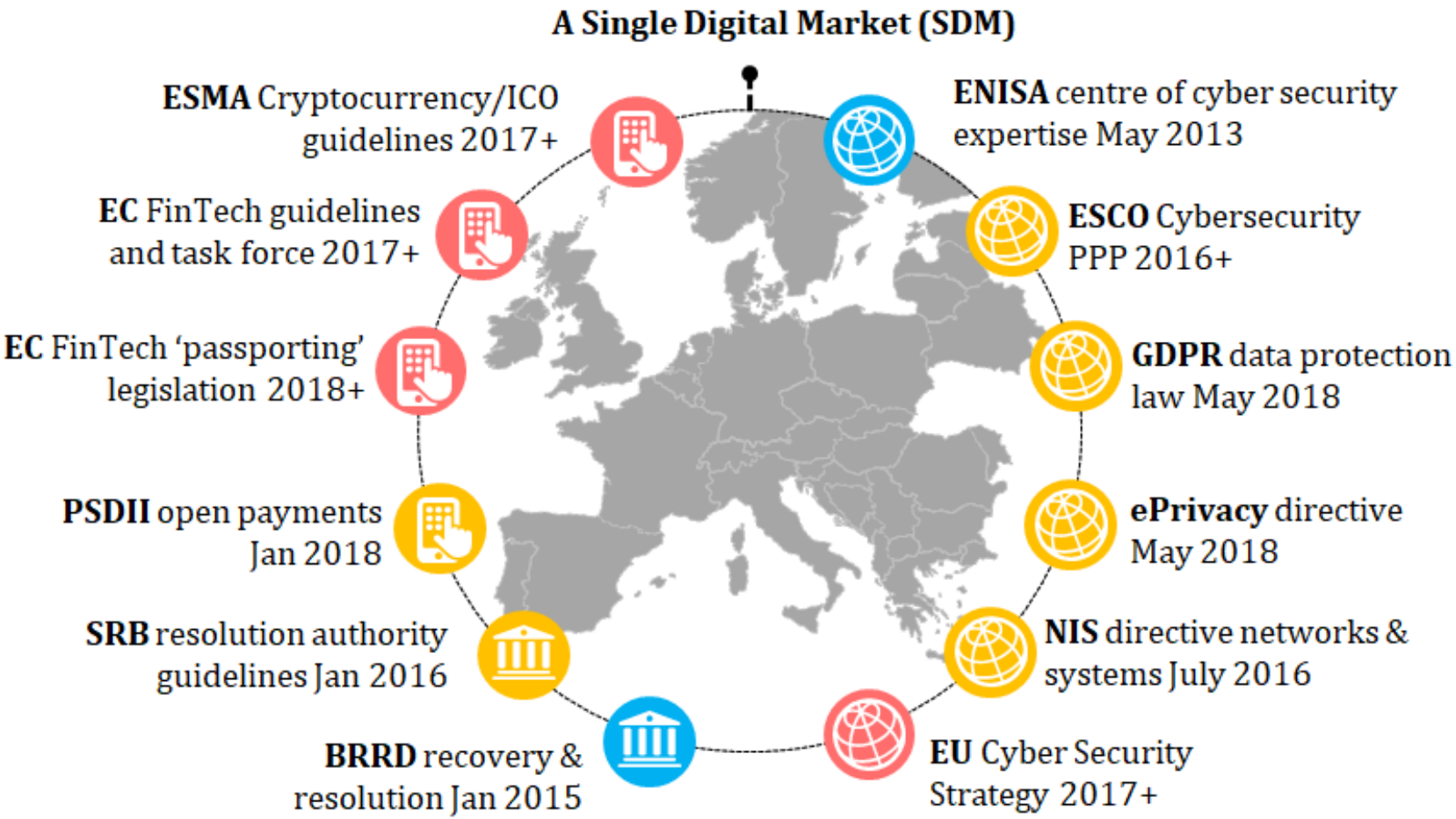
There continues to be challenges on post-crisis returns with high technology and regulatory change costs creating bottom line pressures.

Increasing value and flows of data

- 5 - 6% average ROE forecast for global investment banks[1]
- 83% rise in external cyber threats in financial services from 2015+[2]
- 150+ active DLT proof of concepts underway in financial services in 2017[3]
- $1.2bn raised through Initial Coin Offerings (ICO) in 2017, surpassing Blockchain and Bitcoin[4]

1. EY *Investment Bank of the Future*
2. IBM *2015 Cyber Intelligence*
3. Editionfinancial *Blockchain in FS*
4. Autonomous NEXT *TokenMania*

The Developing EU Policy Framework



A selection of policy shown; not exhaustive.

FinTech and Emerging Technologies

Cyber Security, Data and Protection

Operational Resilience, Resolution and Recovery

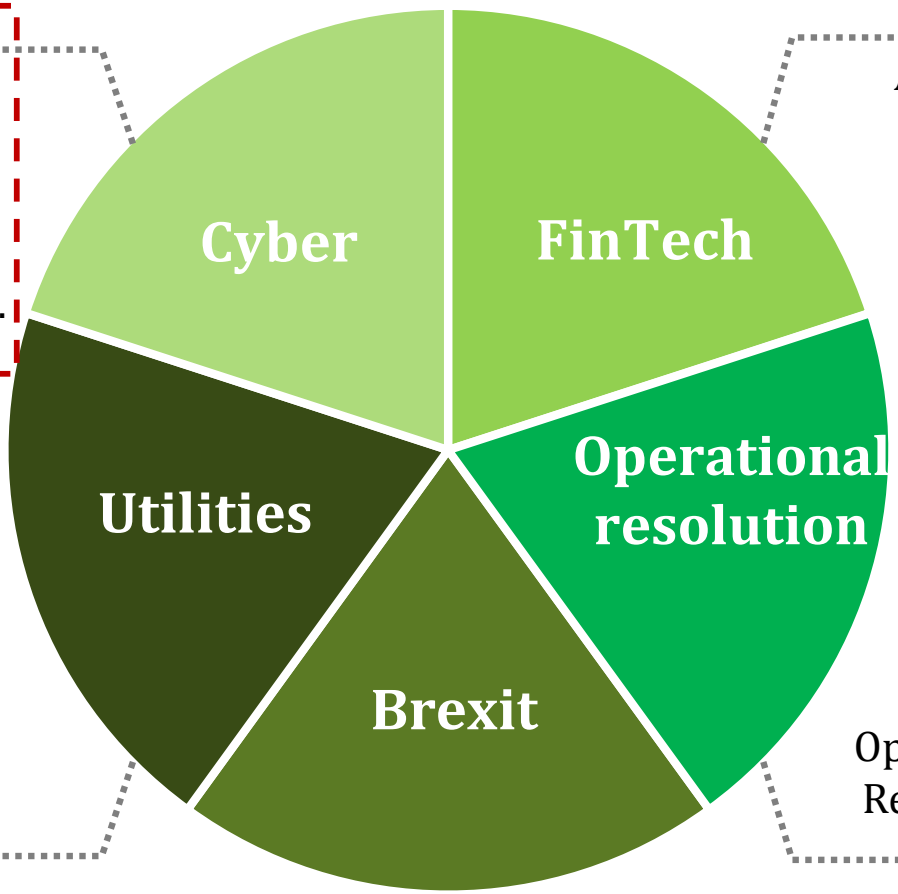
Established

Developing or in implementation

Future watchlist

Areas of Work in the Committee

The threat from cybercrime impacting the industry, and how AFME can promote standards and policy harmonisation.



Accelerating technology innovation and how AFME can contribute and support standards, opportunities, and risks.

The opportunities for increased utility adoption, and how AFME can develop industry best practice guidelines.

To promote harmonisation for Operational Recovery and Resolution requirements.

To identify the operational implications of Brexit and recommendations for policymakers.

afme/ Finance for Europe

Association for Financial Markets in Europe

The Increasing Global Risk of Cyber Attacks

Emmanuel Le Marois, Manager, Technology and Operations, AFME

The Increasing Global Risk of Cyber Attacks

Cyber Attacks pose a major instability risk today

The internet, technology, and devices are increasingly connecting users, firms and the global economy…

…making integrity and resilience a priority.

2020: The Insecurity of Things?
Number of users: 4.1 billion[4]
Connected devices: 20.4 billion[3]
- Autonomous cars
- Medical devices,
- Smart homes
- Industrial equipment monitoring…

- 20 billion devices connected
- More critical infrastructures connected
- Increased attack surface and unpredictability of attacks

2017: Internet of Things (IoT)
Number of users: 3.5 billion[2]
- SMS generates $812,000 per minute
- 85% of population on mobile phones

Connected devices: 8.3 billion[3]

- 3.5 billion internet users
- Critical infrastructures dependent on technology
- Internet availability, integrity and resilience a global priority

1990: world wide web (www) invented
Number of users: 3 million[1]

1969: First "internet" message between two universities
Number of users: 2

1969 1990 2017 2020

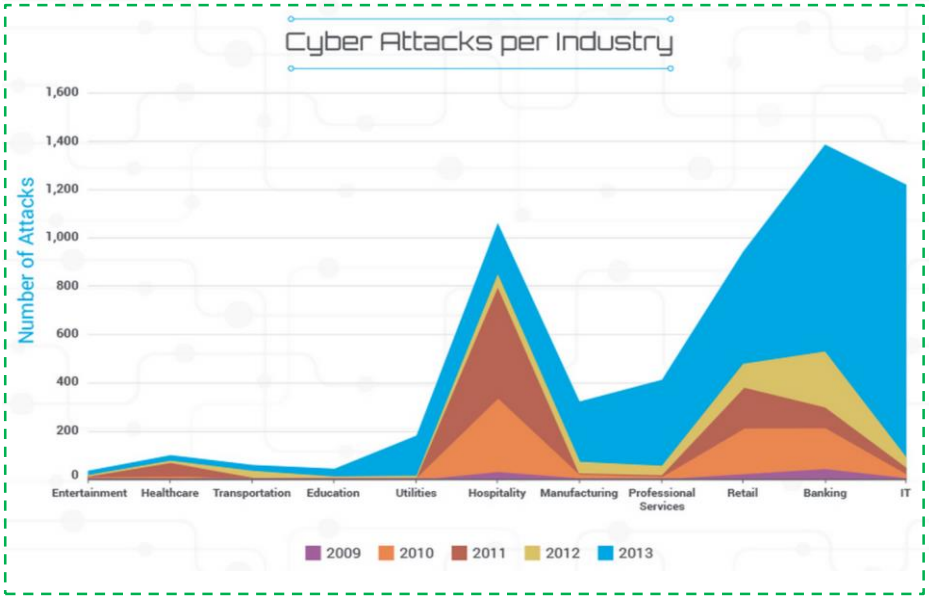
1. World Mapper: Link
2. Statista: Link
3. Gartner: Link
4. Gemalto: Link

The Increasing Global Risk of Cyber Attacks

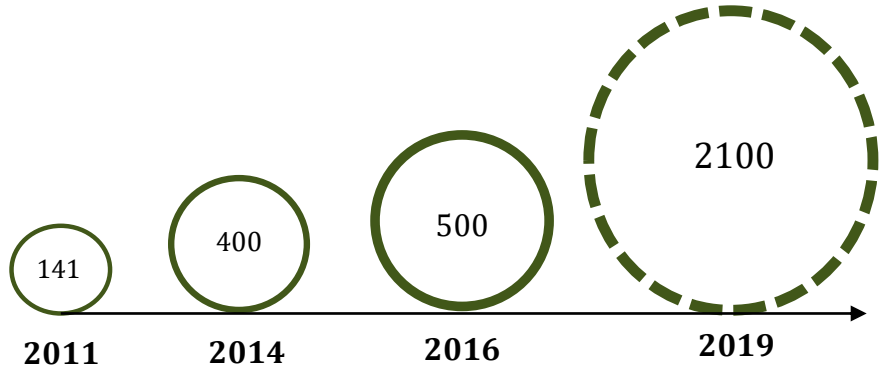
Cyber attacks are increasingly more costly

Across all sectors, the volume of cyber attacks is increasing[1].

Across the globe, the estimated cost of cyber attacks is increasing.



Estimated Cost of Global Cyber Attacks in US$ billions[2]



Leading to an overall increase in spending in cyber security across all sectors and all jurisdictions.

Security spending between 2012-2016[3]

78% Telecommunications

67% Financial Services

53% Oil and Gas

Cybersecurity spending in US$ billions[3]

1. Ponemon Institute: Link
2. McAfee: Link
3. PwC: Link

The Increasing Global Risk of Cyber Attacks

Examples of two recent major cyber attacks

Bangladesh Central Bank

- **Date**: February 2016
- **Target**: Government/Regulators
- **Damage**: Attempt to steal $1bn
- **Modus Operandi**:
  - Detailed understanding of SWIFT infrastructure
  - Bangladesh Bank's credentials stolen
  - Malware deployed to create seemingly genuine SWIFT instruction
- **Success?**
  - $101 million were stolen
- **Lessons Learned:**
  - High degree of sophistication & knowledge
  - Importance of governance, controls and third party risk in cyber security
  - Fundamental review of SWIFT security program

Wannacry Ransomware

- **Date**: May 2017
- **Target**: Global
- **Damage**: +220,000 victims
- **Modus Operandi**: **Global Ransomware Attack**
  - Leveraged previously seen ransomware with NSA leaked vulnerabilities
  - "Pay $300 in Bitcoin or you'll lose all your data!"
- **Success?**
  - +220,000 victims in 150 countries in 2 days
  - Victims included large firms such as: Telefonica (Spain), Fedex, NHS hospital (UK)…
- **Lessons Learned:**
  - High interconnectedness of computers
  - Importance of cyber hygiene's

afme/ Finance for Europe

Association for Financial Markets in Europe

The Challenge of Solving Cyber Globally

Emmanuel Le Marois, Manager, Technology and Operations, AFME
Dave Evans, Director, Cyber Resilience, UBS

The Challenge of Solving Cyber Globally

Cyber Attacks are a global issue

Cyber is everywhere

Mon 12th Dec, 2011

Cybersecurity: A global issue demanding a global approach

Thu 23rd Mar, 2017

The year cybersecurity went mainstream

WORLD ECONOMIC FORUM

Sun 9th Jul, 2017

Putin & I discussed forming an impenetrable Cyber Security unit

Donald J. Trump
@realDonaldTrump

Mon 17th Jul, 2017

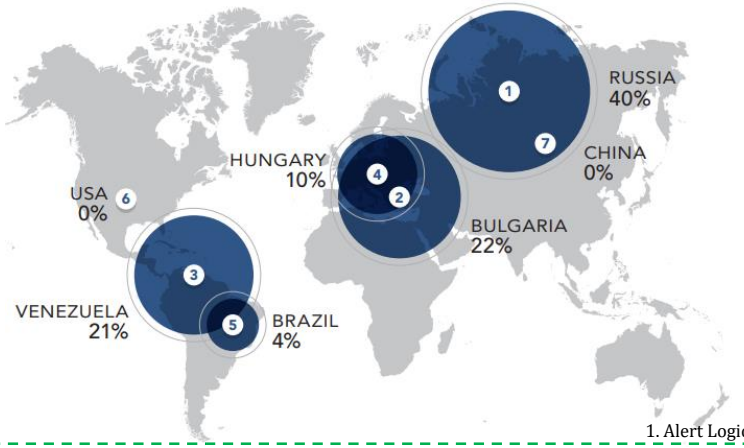
One of the biggest concern for autonomous vehicles is a fleet-wide hack

Sept, 2017

Financial Services face increasingly sophisticated threat actors but also more intense scrutiny from industry regulators

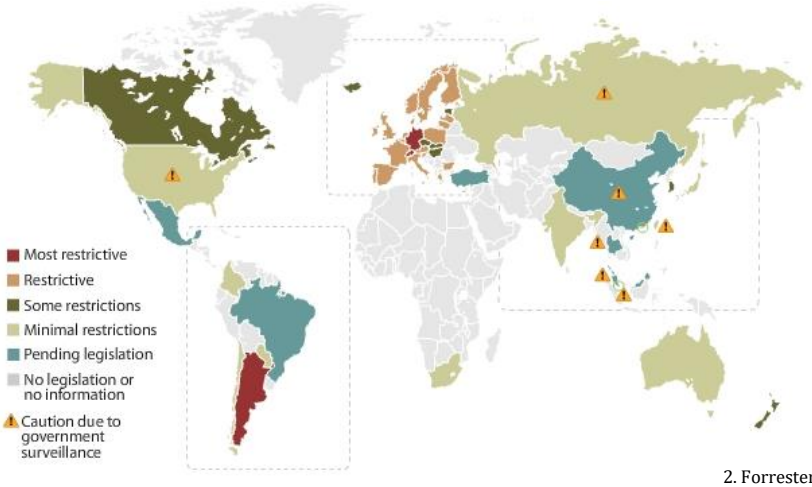
pwc

Cyber attacks originate from multiple jurisdictions affecting firms operating across borders[1].



1. Alert Logic: Link

National regulators are taking action but with disparate laws the cost of compliance is increasing[2].



2. Forrester: Link

The Challenge of Solving Cyber Globally

Global resilience and regulatory harmonisation

Increasing Global Cyber Resilience.

Tools used to increase Cyber Resilience:
Two approaches to test cyber defences globally.

Prevent Breach

- Threat model
- Code review
- Security testing
- Security development lifecycle

- Prevent a Breach: Conduct vulnerability assessments to identify defence weaknesses.

Assume Breach

- War game exercises
- Centralized security monitors
- Live site penetration testing

- Assume a Breach: Conduct penetration tests or attack simulations to assess response.
- Variation: Use live threat information to emulate attack, e.g. Threat Led Penetration testing (TLP).

Coordinating Regulatory Efforts Globally.

Top Down vs Bottom up:
Cyber is a global threat impacting multi-jurisdictional firms. Influential regulators need to coordinate efforts in a Global forum, creating a network effect to harmonise.

afme/ Finance for Europe

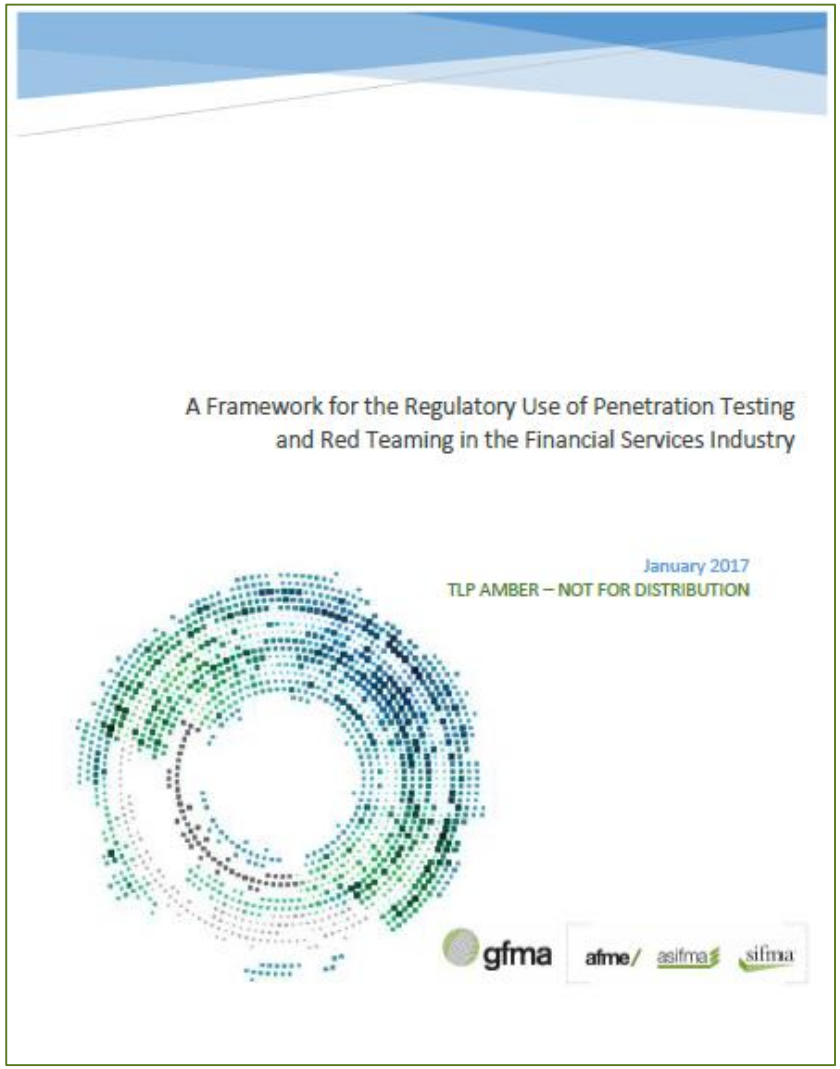
Association for Financial Markets in Europe

GFMA Penetration Testing Framework

Emmauel LeMarois, Manager, Technology and Operations, AFME
Dave Evans, Director, Cyber Resilience, UBS

GFMA Penetration Testing Framework

Overview of the framework



"…Penetration testing serves as one of the foremost tools in enabling a robust security program within a financial institution. Such testing allows firms to evaluate their systems and the controls that protect them in order to identify and remediate vulnerabilities, thereby strengthening their infrastructure against cyber threats…"

- Increased interest by global regulators has led to the creation of regulatory-mandated testing initiatives

- While these tests are important pieces of regulatory oversight **they can present risks to firms and the firms' clients if the test results become public or are inadvertently disclosed or stolen**

GFMA Penetration Testing Framework

Aims and principles of the framework

The framework has been completed to:

- **Address the ever-growing cyber threats** posed by nation-states, terrorist organizations, independent actors
- **Promote cooperation between Banks and regulators** to increase stability and cyber defences
- **Support regulatory efforts on mandated third-party penetration testing programs** ("pen testing"), and red team exercises ("red teaming)

The framework aims to:

- Raise awareness of a growing trend
- Prompt an important dialogue between Financial Services and regulators
- Work to find the appropriate balance, structure and methodology to jointly identify and reduce cyber risks in the financial sector
- Promote a harmonised approach for regulatory-mandated, firm lead penetration testing so as to reduce potential fragmentation, operational risks and in fine less effective cyber defences

The framework is based on Four common principles:

- **Principle 1:** Provide regulators the ability to guide penetration testing programs to meet supervisory objectives
- **Principle 2**: Provide regulators confidence that penetration testing is conducted by certified personnel
- **Principle 3:** Provide regulators transparency into the testing process and results
- **Principle 4:** Ensure testing activities minimize operational risks and sensitive data is controlled by protocols

Thank You For Listening.

Any Questions?

afme/ Offices

Finance for Europe

The Association for Financial Markets in Europe advocates stable, competitive and sustainable European financial markets that support economic growth and benefit society.

London
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom

Tel: +44 (0)20 3828 2700

Brussels
Rue de la Loi 82
1040 Brussels
Belgium

Tel: +32 (0)2 788 3971

Frankfurt
Skyper Villa
Taunusanlage 1
60329 Frankfurt am Mai
Germany

Tel: +49 (0)69 5050 60 590

www.afme.eu