Payments 2.0: the new security challenges and role of the European Banking Authority

Geoffroy Goffinet
Consumer Protection, Financial Innovation and Payments

Regional Seminar on Cyber Preparedness – Vienna 18-19 MAy
Outline of the presentation

Introduction to the EBA

> The creation of the EBA
> The European System of Financial Supervision
> Decision making bodies
> Main objective and mandate of the EBA
> EU Directives in the EBA’s scope of action
> Legal instruments available

The new security challenges and EBA’s regulatory work on payments

> Virtual Currencies
> EBA Guidelines on the Security of Internet Payments
> Payment Services Directive 2
Introduction to the EBA
The creation of the EBA

> The EBA was established by Regulation (EC) No. 1093/2010 of the European Parliament and EU Council;

> came into being on 1 January 2011;

> took over all existing tasks and responsibilities from the Committee of European Banking Supervisors (CEBS);

> took on additional tasks, incl. consumer protection and monitoring financial innovation;

> is an independent authority;

> is accountable to the EU Parliament and Council;

> has as its highest governing body the EBA Board of Supervisors, comprising the Heads of the 28 national supervisors.
The European System of Financial Supervision

The EBA is part of the wider system of the European System of Financial Supervision (ESFS).
Main objective and mandate of the EBA

Objective

“To protect the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses.” (Art. 1(5)).

Means by which the EBA is to achieve its objective

The EBA shall inter alia “contribute to

> improving the functioning of the internal market, including in particular, a sound, effective and consistent level of regulation and supervision;

> ensuring the taking of credit and other risks are appropriately supervised and regulated;

> enhancing customer protection.” (Art. 1(5)(f);

> “monitor[ing] new and existing financial activities and adopt[ing] guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice”. (Art. 9)
EU Directives that fall in EBA’s scope of action

The EBA’s scope of action is defined by the EU Directives and Regulations that are listed in Article 1(2) of the EBA’s founding regulation, as well as any future EU Directive, Regulation or Decision that confers tasks on the EBA.

> Capital Requirements Directive (CRD/R IV)
> Bank Recovery and Resolution Directive (BRRD)
> Mortgage Credit Directive (MCD)
> Anti–Money Laundering Directive (AMLD)
> Payment Accounts Directive (PAD)
> Electronic Money Directive (EMD)
> Payment Services Directive (PSD1 + forthcoming PSD2)
> Markets in Financial Instruments Directive (MiFID/R, for structured deposits)
> Interchange Fee Regulation (IFR)
> ....
Legal instruments available to the EBA

The EBA has different types of legal instruments at its disposal. So far, the EBA has issued more than 100 of these instruments.

> Technical standards
> Guidelines and recommendations
> Opinions / Technical Advice
> Warnings
> Temporary prohibitions
> Joint Positions
> Breach of Union law investigations
> Binding and non-binding mediation
Key stakeholders in the policy making process

Policy development on consumer protection and financial innovation at the EBA involves numerous key stakeholders, at various stages of the process.

EBA
- Comprises firms, consumers, SMEs, employees, etc.
- Provides opinions and comments on EBA work
- May suggest issues to be examined by the EBA
- Provides interface with other user groups

Consumer Associations
- May suggest consumer issues to be examined by the EBA
- Provide input and expertise in specific areas

EBA Banking Stakeholder Group
- Established the EBA’s objectives & tasks through EBA founding regulation
- May assign additional tasks through Directives and Regulations
- EU Commission attends EBA BoS and other meetings
- May be the addressee of EBA Opinions and advice

Firms and Trade Associations
- Respond to mandatory EBA impact assessment
- Provide input and expertise in specific areas

EU Commission, Council & Parliament
The new security challenges and EBA’s regulatory work on payments
(I) EBA Opinion on virtual currencies

In June 2014, the EBA published an Opinion addressed to national supervisors and EU co-legislators with an assessment of relevant regulatory aspects.

1. Definition of virtual currencies and market participants

2. Potential benefits

3. Risks, and their causal drivers
   - Risks to users
   - Risks to non-user market participants
   - Risks to financial integrity
   - Risks to payment systems and payment service providers in fiat currencies
   - Risks to regulatory authorities

4. The potential regulatory approach
   - Summary of the key risk drivers
   - A potential regulatory approach for the long term
   - The immediate regulatory response for the short term
Potential benefits of virtual currencies

The EBA assessed a number of benefits that virtual currencies are said to deliver.

1. Reduction in transaction costs
2. Reduction of transaction processing time
3. Contribution to economic growth
4. Financial inclusion
5. Security of personal data
Risks

The EBA identified 70+ risks, to users, non-user market participants, financial integrity, fiat currency payment systems, as well as to regulatory authorities.
The short regulatory response

Until a potential long-term regulatory approach is in place, the regulated financial system needs to be ‘shielded’ from virtual currency schemes.

- National supervisory authorities should discourage regulated financial institutions from buying, holding or selling VCs;

- VCs can continue to innovate (including to develop solutions that satisfy potential regulatory requirements) but need to do so outside of the financial services sector; and

- EU co-legislators should consider declaring virtual currency exchanges as ‘obliged entities’ under the AMLD, which would require them to comply with AML and CTF requirements.
A potential regulatory approach for the long-term

In order to address the risk drivers, a regulatory approach would be required with numerous components, which will take some time to develop.

A. Mandatory establishment of ‘scheme governance authorities’
B. Customer due diligence (CDD) requirements
C. Fitness and probity standards
D. Mandatory incorporation
E. Transparent price formation & requirements against market abuse
F. Authorisation and corporate governance
G. Capital requirements
H. Separation of client accounts
I. Evidence of secure IT systems
J. Payment guarantee and refunds
K. Separation of VC schemes from conventional payment systems
L. Miscellaneous requirements
II. EBA Guidelines on security of internet payments

On 18 December 2014, the EBA published final Guidelines on the security of internet payments (EBA/GL/2014/12).

- represents first output of joint work carried out by ECB & EBA on security of retail payments;
- based on SecuRe Pay recommendations of January 2013;
- issued in order to ensure a consistent regulation across the EU and provide legal certainty for market participants;
- comprises three sets of requirements, related to:
  - the general control and security environment
  - specific control and security measured for internet payments
  - customer awareness, education and communication
- have to be implemented by 1 August 2015;
- national authorities are currently submitting compliance notifications;
- will be in force until enhanced requirements come into effect as a result of the forthcoming PSD2 (estimated to be effective from 2017/18).
III. EBA mandates in the PSD2

The negotiations suggest that the PSD2 will confer a number of roles on EBA among which security related issues.

A. Defining security requirements for electronic payments
   - Art. 85: GL on implementing/monitoring of security measures
   - Art. 87a: Common and secure requirements for communication for the purpose of authentication, notification and information as well as the requirements to protect the confidentiality and the integrity of the payment service users’ personalised security credentials

B. Improving incident reporting throughout the European Union
   - Art. 86: CAs to provide details of incidents to EBA and ECB;
   - Art. 86: Guidelines on classification, content, format and criteria for reporting;

➢ EBA will start formally to engage with market participants once PSD2 text is final.