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

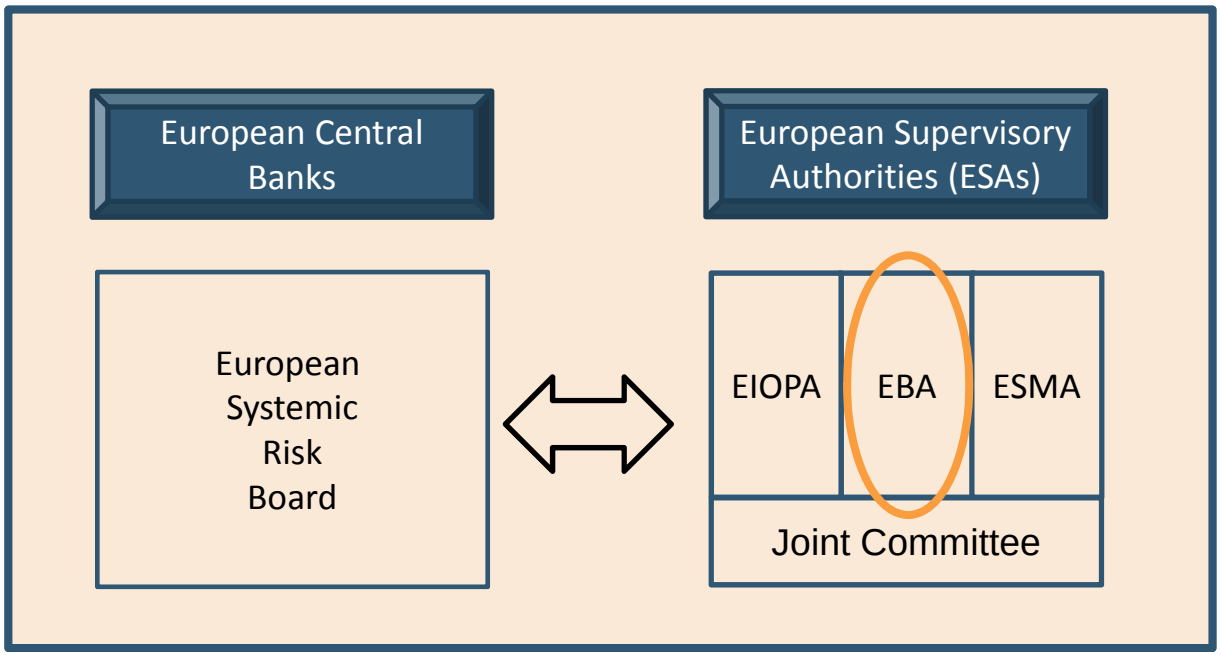
Introduction to the EBA

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).

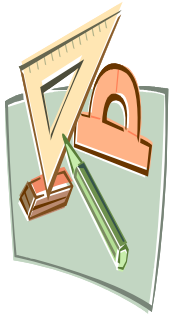


Main objective and mandate of the EBA

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

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

Consumer Associations

> 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

EBA Banking Stakeholder Group

> Respond to mandatory EBA impact assessment
> Provide input and expertise in specific areas

Firms and Trade Associations

> Established the EBA's objectives & tasks though 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

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.

		ID	Risk description	Rank
A) Risks to users	General risks, irrespective of purpose	A01	User suffers loss when an exchange is fraudulent	High
		A02	User suffers loss when an ostensible exchange is not a genuine exchange	High
		A03	User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation	High
		A04	User holding VCs may unexpectedly become liable to tax requirements	Med
		A05	User who is a member of a VC mining pool does not get fair share of mined VC units from a mining consortium	Low
		A06	User suffers loss when buying VCs that do not have the VC features that the user expects	Med
		A07	User's computing capacity is abused for the mining benefit of others	Low
		A08	User suffers loss due to changes made to the VC protocol and other core components	High
		A09	User is not in a position to identify and assess the risks arising from VCs	Low
		A10	User is in violation of applicable laws and regulations	Med
		A11	User loses VC units through e-wallet theft or hacking	High
		A12	User loses VC units when exchange gets hacked	High
		A13	User's identity may be stolen when providing identification credentials to access VCs	High
		A14	Market participants suffer losses due to unexpected application of law that renders contracts illegal/unenforceable	Med
		A15	Market participants suffer losses due to delays in the recovery of VC units or the freezing of positions	High
		A16	Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations	High
		A17	Market participants suffer losses of VC units held in custody by others	Med
		A18	Market participants suffer losses through information inequality regarding other actors	Med
	When used as a means of payment	A21	User suffers loss when counterparty fails to meet contractual payment or settlement obligations	High
		A22	User experiences fraud or loss of FC when using VC cash machines	Med
		A23	User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis	High
		A24	User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet	High
		A25	User is not able to convert VCs into fiat currency, or not at a reasonable price	High
		A26	User is unable to access VCs after losing passwords/keys to their e-wallet	High
		A27	User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate)	High
		A28	User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate)	High
	When used as an investment	A41	User suffers loss as a result of VC prices being manipulated	High
		A42	User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss	Med
		A43	User is misled by unreliable exchange rate data	Med
		A44	User suffers loss when investing in fraudulent VC investment schemes	Med
		A45	User is exposed to significant price volatility within very short time frames	Med
		A46	User cannot execute the VC exchange at the expected price	Med
		A47	User is exploited by a VC Ponzi scheme	Med
B) Risks to non-user market participants	Specific to exchanges	B11	Exchange is operationally unable to fulfil payment obligations denominated in VCs or FCs	Med
		B12	Exchange is not in control of its operation	Med
		B13	E-wallet provider faces loss should their refund policies be abused to hedge currency transactions	Med
	Specific to merchants	B21	After accepting VC for payment, merchant is not reimbursed	Med
		B22	Unlike a FC, the merchant cannot be certain that they can spend the VCs received	Med
		B23	The merchant cannot be certain of the FC purchasing power of the VCs they have received	Med
		B24	Merchant faces compensation claims from customers if transactions have been wrongly debited	Med
	Specific to some other market participants	B31	Wallet provider loses e-wallets provided for individuals	High
		B32	Scheme governance authority fails to meet payment and other obligations	High
		B33	Scheme governance authority is subject to unexpected civil/criminal liability that brings the VC scheme to a halt	Med
		B34	E-wallet provider faces compensation claims from customers if functionality of wallet is compromised or fails to provide expected functionality	Med

			Risk description	Rank
C) Risks to financial integrity	Money laundering and terrorist financing	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med
D) Risks to payment systems in FCs		D01	Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal	Low
		D02	PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations	Low
		D03	PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated	Med
		D04	Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc.	Low
E) Risks to regulatory authorities	Reputation risks	E01	Regulators decide to regulate VCs but the chosen regulatory approach fails	Med
		E02	Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs	Med
		E03	Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks	Med
	Legal	E11	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable	Low
	Risks to competition objectives	E21	Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge	Med
		E22	If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets	Med
		E23	Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive	Med
	To authority issuing FC (out of scope of	E31	Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict	Low

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.**