Antitrust: Commission fines Barclays, RBS, Citigroup, JPMorgan and MUFG €1.07 billion for participating in foreign exchange spot trading cartel

In two settlement decisions, the European Commission has fined five banks for taking part in two cartels in the Spot Foreign Exchange market for 11 currencies – Euro, British Pound, Japanese Yen, Swiss Franc, US, Canadian, New Zealand and Australian Dollars, and Danish, Swedish and Norwegian crowns.

The first decision (so-called "Forex – Three Way Banana Split" cartel) imposes a total fine of €811 197 000 on Barclays, The Royal Bank of Scotland (RBS), Citigroup and JPMorgan.

The second decision (so-called "Forex- Essex Express" cartel) imposes a total fine of €257 682 000 on Barclays, RBS and MUFG Bank (formerly Bank of Tokyo-Mitsubishi).

UBS is an addressee of both decisions, but was not fined as it revealed the existence of the cartels to the Commission.

Commissioner Margrethe **Vestager**, in charge of competition policy said:*"Companies and people depend on banks to exchange money to carry out transactions in foreign countries. Foreign exchange spot trading activities are one of the largest markets in the world, worth billions of euros every day. Today we have fined Barclays, The Royal Bank of Scotland, Citigroup, JPMorgan and MUFG Bank and these cartel decisions send a clear message that the Commission will not tolerate collusive behaviour in any sector of the financial markets. The behaviour of these banks undermined the integrity of the sector at the expense of the European economy and consumers".*

Foreign Exchange, or "Forex", refers to the trading of currencies. When companies exchange large amounts of a certain currency against another, they usually do so through a Forex trader. The main customers of Forex traders include asset managers, pension funds, hedge funds, major companies and other banks.

Forex spot order transactions are meant to be executed on the same day at the prevailing exchange rate. The most liquid and traded currencies worldwide (five of which are used in the European Economic Area) are the Euro, British Pound, Japanese Yen, Swiss Franc, US, Canadian, New Zealand and Australian Dollars, and Danish, Swedish and Norwegian crowns.

The Commission's investigation revealed that some individual traders in charge of Forex spot trading of these currencies on behalf of the relevant banks exchanged sensitive information and trading plans, and occasionally coordinated their trading strategies through various online professional

chatrooms.

The commercially sensitive information exchanged in these chatrooms related to:

1) outstanding customers' orders (i.e. the amount that a client wanted to exchange and the specific currencies involved, as well as indications on which client was involved in a transaction),

2) bid-ask spreads (i.e. prices) applicable to specific transactions,

3) their open risk positions (the currency they needed to sell or buy in order to convert their portfolios into their bank's currency), and

4) other details of current or planned trading activities.

The information exchanges, following the tacit understanding reached by the participating traders, enabled them to make informed market decisions on whether to sell or buy the currencies they had in their portfolios and when.

Occasionally, these information exchanges also allowed the traders to identify opportunities for coordination, for example through a practice called "standing down" (whereby some traders would temporarily refrain from trading activity to avoid interfering with another trader within the chatroom).

Most of the traders participating in the chatrooms knew each other on a personal basis – for example, one chatroom was called *Essex Express 'n the Jimmy* because all the traders but "James" lived in Essex and met on a train to London. Some of the traders created the chatrooms and then invited one another to join, based on their trading activities and personal affinities, creating closed circles of trust.

The traders, who were direct competitors, typically logged in to multilateral chatrooms on Bloomberg terminals for the whole working day, and had extensive conversations about a variety of subjects, including recurring updates on their trading activities.

The Commission's investigation revealed the existence of two separate infringements concerning foreign exchange spot trading:

– The *Three Way Banana Split* infringement encompasses communications in three different, consecutive chatrooms *("Three way banana split / Two and a half men / Only Marge"*) among traders from UBS, Barclays, RBS, Citigroup and JPMorgan. The infringement started on 18 December 2007 and ended on 31 January 2013.

– The *Essex Express* infringement encompasses communications in two chatrooms ("*Essex Express 'n the Jimmy*" and "*Semi Grumpy Old men*") among traders from UBS, Barclays, RBS and Bank of Tokyo-Mitsubishi (now MUFG Bank). The infringement started on 14 December 2009 and ended on 31 July 2012.

The following table details the participation and the duration of each company's involvement in each of the two infringements:

	Company	Start	End
Three Way Banana Split / Two and a half men/ Only Marge	UBS	10/10/2011	31/01/2013
	Barclays	18/12/2007	01/08/2012
	RBS	18/12/2007	19/04/2010
	Citigroup	18/12/2007	31/01/2013
	JP Morgan	26/07/2010	31/01/2013
Essex Express / Semi Grumpy Old men	UBS		
	Barclays	14/12/2009	31/07/2012
	RBS	14/12/2009	31/07/2012
	Bank of Tokyo-Mitsubishi (now MUFG Bank)	14/09/2010 08/09/2010	08/11/2011 12/09/2011

Fines

The fines were set on the basis of the Commission's 2006 Guidelines on fines (see also MEMO).

In setting the fines, the Commission took into account, in particular, the sales value in the European Economic Area (EEA) achieved by the cartel participants for the products in question, the serious nature of the infringement, its geographic scope and its duration.

Under the Commission's 2006 Leniency Notice:

- UBS received full immunity for revealing the existence of the cartels, thereby avoiding an aggregate fine of ca. €285 million.
- In the *Three Way Banana Split* infringement, all banks involved benefited from reductions of their fines for their cooperation with the Commission investigation. The reductions reflect the timing of their cooperation and the extent to which the evidence they provided helped the Commission to prove the existence of the cartel in which they were involved.
- In the *Essex Express* infringement, all banks except one benefited from reductions of their fines for their cooperation with the Commission investigation. The reductions reflect the timing of their cooperation and the extent to which the evidence they provided helped the Commission to prove the existence of the cartels in which they were involved. MUFG Bank (formerly Bank of Tokyo-Mitsubishi) did not apply for leniency.

In addition, under the Commission's 2008 Settlement Notice, the Commission applied a reduction of 10% to the fines imposed on the companies in view of their acknowledgment of participation in the cartels and of their liability in this respect.

The breakdown of the fines imposed on each company is as follows:

THREE WAY BANANA SPLIT

Company	Reduction under Leniency Notice	Reduction under Settlement Notice	Fine (€)
UBS	100%	10%	0
Barclays	50%	10%	116 107 000
RBS	30%	10%	155 499 000
Citigroup	20%	10%	310 776 000
JPMorgan	10%	10%	228 815 000
TOTAL			811 197 000

ESSEX EXPRESS

Company	Reduction under Leniency Notice	Reduction under Settlement Notice	Fine (€)
UBS	100%	10%	0
Barclays	50%	10%	94 217 000
RBS	25%	10%	93 715 000
BOTM		10%	69 750 000
TOTAL			257 682 000

Procedural Background

Article 101 of the Treaty on the Functioning of the European Union (TFEU) and Article 53 of the EEA Agreement prohibit cartels and other restrictive business practices.

The Commission's investigation in this case started in September 2013, with an immunity application under the Commission Leniency Notice submitted by UBS, which was followed by applications for reduction of fines by other parties.

The Commission will continue pursuing other ongoing procedures concerning past conduct in the Forex spot trading market.

Fines imposed on companies found in breach of EU antitrust rules are paid into the general EU budget. This money is not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly. The fines therefore help to finance the EU and reduce taxpayers' contributions.

More information on this case will be available under the case number AT.40135 in the public case register on the Commission's competition website, once confidentiality issues have been dealt with. For more information on the Commission's action against cartels, see its cartels website.

The settlement procedure

Today's decisions are the 30th and 31st settlement decisions since the introduction of the settlement procedure for cartels in June 2008 (see press release and MEMO). In a settlement, companies acknowledge their participation in a cartel and their liability for it. Settlements are foreseen in Antitrust Regulation 1/2003 and allow the Commission to apply a simplified and shortened procedure. This benefits consumers and taxpayers as it reduces costs. It also benefits antitrust enforcement as it frees up resources to tackle other suspected cartels. Finally, the companies themselves benefit in terms of quicker decisions and a 10% reduction in fines.

Action for damages

Any person or company affected by anti-competitive behaviour as described in this case may bring the matter before the courts of the Member States and seek damages. The case law of the Court and Council Regulation 1/2003 both confirm that in cases before national courts, a Commission decision constitutes binding proof that the behaviour took place and was illegal. Even though the Commission has fined the cartel participants concerned, damages may be awarded without being reduced on account of the Commission fine.

The Antitrust Damages Directive, which Member States had to implement by 27 December 2016, makes it easier for victims of anti-competitive practices to obtain damages. More information on antitrust damages actions, including a practical guide on how to quantify antitrust harm, is available here.

Whistleblower tool

The Commission has set up a tool to make it easier for individuals to alert it about anti-competitive behaviour while maintaining their anonymity. The tool protects whistleblowers' anonymity through a specifically-designed encrypted messaging system that allows two way communication. The tool is accessible via this link.

March 2019 – Euro area international trade in goods surplus €22.5 bn – €2.9 bn surplus for EU28

The first estimate for euro area (EA19) exports of goods to the rest of the world in March 2019 was €205.6 billion, an increase of 3.1% compared with March 2018 (€199.5 bn). Imports from the rest of the world stood at €183.1 bn, a rise of 6.0% compared with March 2018 (€172.7 bn).

Full text available on EUROSTAT website

Sweden: European backing for Northvolt's battery gigafactory

- **In principle approval of the European Investment Bank to support Northvolt's gigafactory for lithium-ion battery cells in Skellefteå, Sweden.**
- **Pending finalisation of due diligence and negotiations, the EIB's financing commitment is foreseen to be EUR 350 million.**

The European Investment Bank has given its in-principle agreement to support the financing of Europe's first home-grown gigafactory for lithium-ion battery cells, *Northvolt Ett*, in Sweden. Upon conclusion of a loan agreement, the financing would be supported by the European Fund for Strategic Investments (EFSI), the main pillar of the Investment Plan for Europe.

The gigafactory will be established in Skellefteå in northern Sweden – a region home to a prominent raw material and mining cluster which has a long history of process manufacturing and recycling. Noting the region's clean power base, building the factory in northern Sweden will enable Northvolt to utilise 100% renewable energy within its production processes.

EIB Vice-President **Andrew McDowell** noted: "*The development of a competitive and green battery value chain within Europe can not only cut greenhouse gas emissions by decarbonising power generation and transport, but can also help protect millions of well paid jobs in European industries in the face of increasing global competition. The EUR 350m loan to Northvolt approved in-principle today by our Board of Directors is the largest ever direct EIB financing approval for battery technology, and we look forward to working with Northvolt over the coming months to finalise contracts.*"

Maroš Šefčovič, European Commission Vice-President for the Energy Union, said *"The EIB and the Commission are strategic partners under the EU Battery Alliance. I welcome the significant support proposed by the EIB to Northvolt gigafactory as a stepping-stone towards building a competitive, sustainable and innovative value chain, with battery cells manufactured at scale, here, in Europe. Our two institutions are working closely with the industry and key Member States to put the EU on a firm path towards global leadership in this rapidly expanding sector".*

Northvolt Ett will serve as Northvolt's primary production site, hosting active material preparation, cell assembly, recycling and auxiliaries. The construction of the first quarter of the factory will be completed in 2020. Ramping up to full capacity, *Northvolt Ett* will produce 32 GWh of battery capacity per year.

“*This EIB in principle approval is a key moment in the process of finalizing our capital raise to support the establishment of Northvolt Ett. Today, we are one step closer to our goal of building the greenest batteries in the world and enabling the European transition to a decarbonized future*.” said **Peter Carlsson**, Co-founder and CEO of Northvolt.

The capital raise, in which this EIB loan would be included, will finance the establishment of the first 16 GWh of battery capacity production. The batteries from *Northvolt Ett* are targeted for use in automotive, grid storage, and industrial and portable applications.

“*Today’s decision by the EIB is very gratifying and a big step towards a large-scale battery production in the EU and a fossil free welfare society. The decision shows that there are prerequisites in Sweden for sustainable battery production, it is important for Sweden and the rest of the EU to produce battery materials and battery cells, based on green, Swedish electricity*”, said **Ibrahim Baylan**, Swedish Minister for Business, Industry and Innovation

---

2019-05-16

16 May 2019

In an unprecedented, international law enforcement operation, a complex, globally operating and organised cybercrime network was dismantled. The criminal network used GozNym malware to steal an estimated $100 million from more than 41 000 victims, primarily businesses and their financial institutions.

A criminal indictment returned by a federal grand jury in Pittsburgh, USA, charged 10 members of the GozNym criminal network with conspiracy to commit the following:

- infect victims’ computers with GozNym malware designed to capture victims’ online banking login credentials;
- use the captured login credentials to fraudulently gain unauthorised access to victims’ online bank accounts;
- steal money from victims’ bank accounts and laundering those funds using US and other beneficiary bank accounts controlled by the defendants.

The international law enforcement operation initiated criminal prosecutions against members of the network in four different countries. During the course of the operation, searches were conducted in Bulgaria, Georgia, Moldova and Ukraine. Criminal prosecutions have been initiated in Georgia, Moldova, Ukraine and the United States.

This operational success is a result of the international law enforcement

cooperation between participating EU Member States (Bulgaria and Germany) as well as Georgia, Moldova, Ukraine and the United States (in alphabetical order). Europol, the European Agency for Law Enforcement Cooperation as well as Eurojust, the European Union's Judicial Cooperation Unit supported the case. This operation showcases how an international effort to share evidence and initiate criminal prosecutions can lead to successful results in multiple countries.

Cybercrime as a service

The GozNym network exemplified the concept of 'cybercrime as a service' with different criminal services, such as cyberattacks, bulletproof 'hosters', money mule networks, 'crypters', spammers, coders, organisers, and technical support.

The defendants advertised their specialised technical skills and services on underground, Russian-speaking online criminal forums. The GozNym network was formed when these individuals were recruited from the online forums by the GozNym leader, who controlled more than 41 000 victim computers infected with GozNym malware. The leader of the GozNym criminal network and his technical assistant are being prosecuted in Georgia by the Prosecutor's Office of Georgia and the Ministry of Internal Affairs of Georgia.

Highly specialised and international criminal network

- A member of the network who encrypted GozNym malware to enable it to avoid detection by antivirus tools and protective software on victims' computers is being prosecuted in Moldova by the Prosecutor General and the General Police Inspectorate of the Republic of Moldova.
- Another member from Bulgaria was already arrested by the Bulgarian authorities and extradited to the United States in December 2016 to face prosecution. His primary role in the conspiracy was that of a 'casher' or 'account takeover specialist' who used victims' stolen online banking credentials, captured by GozNym malware, to access victims' online bank accounts and attempt to steal their victims.
- Several members of the network provided money laundering services and were known as 'cash-outs' or 'drop masters'. These individuals, including two from Russia and one from Ukraine, provided fellow members of the conspiracy with access to bank accounts they controlled, which were designated to receive stolen funds from GozNym victims' online bank accounts.
- Five Russian nationals charged in the indictment remain on the run. In addition to the two 'drop masters' referenced above, the group of these defendants includes the developer of the GozNym malware who oversaw its creation, development, management and leasing to other cybercriminals.
- One of the Russian GozNym members conducted spamming operations on behalf of the network. The spamming operations involved the mass distribution of GozNym malware through 'phishing' emails. Those emails were designed to appear legitimate to entice the recipients to open them

and click on a malicious link or attachment that facilitated the downloading of GozNym onto the victims' computers.
- Another Russian-born member of the network was a 'casher' or 'account takeover specialist' who resided in Ukraine at the time of the attacks. Like the Bulgarian defendant, he used victims' stolen online banking credentials captured by GozNym malware to access victims' online bank accounts and attempt to steal victims' money through electronic fund transfers into bank accounts controlled by fellow conspirators.

Avalanche network

Bulletproof hosting services were provided to the GozNym criminal network by an administrator of the service known as the 'Avalanche' network. The Avalanche network provided hosting services to more than 200 cybercriminals, and hosted more than twenty different malware campaigns, including GozNym. At the request of the United States and Germany, the administrator's apartment in Poltava, Ukraine, was searched in November 2016, during an operation led by Germany to dismantle the network's servers and other infrastructure. Through the coordinated efforts being announced today, this notorious cybercriminal will now face prosecution in Ukraine for his role in providing bulletproof hosting services to the GozNym criminal network. The prosecution will be conducted by the Prosecutor General's Office (PGO) and the National Police of Ukraine.

The operation was conducted by the United States Attorney's Office for the Western District of Pennsylvania, the Federal Bureau of Investigation (FBI)'s Pittsburgh Field Office, the Public Prosecutor's Office (PPO) Verden (Germany), the PPO of Georgia, PGO of Ukraine, the Office of the Prosecutor General of the Republic of Moldova, the PGO of Bulgaria, the German Lüneburg Police, the Ministry of Internal Affairs of Georgia, the National Police of Ukraine, the General Police Inspectorate of the Republic of Moldova, and Bulgaria's General Directorate for Combatting Organised Crime. Europol and Eurojust played a critical role in supporting this coordinated law enforcement operation. The Office of International Affairs of the US Department of Justice provided significant assistance.

Eurojust, the EU's Judicial Cooperation Unit, facilitated the investigations by holding coordinating meetings, helping with the exchange of information and judicial best practice, and providing financial support and translation services. The successful result of the operation was also due to the active role of the Liaison Prosecutors from the United States and Ukraine appointed to Eurojust, as well as to the experience and expertise of the European Judicial Cybercrime Network, which is hosted at Eurojust since 2016.

Defence cooperation: Council assesses progress made in the framework of PESCO after first year of implementation

The Council today discussed PESCO after its **first full year of implementation.** It adopted a recommendation **assessing the progress made** by the participating member states to fulfil commitments undertaken in the framework of Permanent Structured Cooperation (PESCO).

The Council underlines that participating member states have **made progress in increasing the level of defence budgets and joint defence investment** with an increase of the aggregated defence budgets of 3.3% in 2018 and 4.6% 2019. Another positive trend is the fact that participating member states are increasingly **using EU tools, initiatives and instruments in national defence planning**, such as the revised Capability Development Plan (CDP), the Coordinated Annual Review for Defence (CARD) and the European Defence Industrial Development Programme (EDIDP). They have started preparing for the European Defence Fund which should replace the EDIDP for the period 2021-2027.

The Council invites participating member states to continue to make progress in fulfilling the more binding commitments related to bringing their respective defence systems more in line with each other, in particular **to strengthen collaborative capability development.** It also encourages them to make further efforts as regards the commitments related to **strengthening the availability and deployability of forces**, including for military Common and Security Defence Policy (CSDP) operations and missions.

Participating member states are also encouraged to advance the work and **focus on the swift and effective implementation of the 34 PESCO projects** in which they participate in order to deliver tangible outputs and products. As a high number of PESCO projects respond to EU capability development priorities which also reflect NATO priorities, **coherence between EU and NATO** respective processes will continue to be ensured. The recommendation also foresees that after 2019, the next call for PESCO projects would take place in 2021.

Background

The Council adopted a decision establishing Permanent Structured Cooperation (PESCO) on 11 December 2017. PESCO enables participating EU member states to work more closely together in the area of security and defence. This permanent framework for defence cooperation allows willing and able member states to develop jointly defence capabilities, invest in shared projects, and enhance the operational readiness and contribution of their armed forces.

The Council agreed on 17 initial projects on 11 December 2017 and formally

adopted them on 6 March 2018. The Council adopted 17 additional projects on 11 November 2018. The projects cover areas such as training, capability development and operational readiness on land, at sea and in the air, as well as cyber-defence.

The 25 member states participating in PESCO are: Austria, Belgium, Bulgaria, Czech Republic, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Spain and Sweden.

Visit the meeting page