Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, 27. November 2015

France's contribution

New efforts to combat terrorist financing at European level

Terrorist attacks on European soil in recent years have underscored the need to substantially boost efforts to fight terrorism and terrorist financing at EU level.

The adoption of the AML package, consisting of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing – the so-called Fourth anti-money laundering Directive – and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, represented a first step in stepping up European legislation to combat terrorist financing. Under the present circumstances, it is imperative to step up enactment of this package in every EU Member State so that it enters into force much earlier than the original June 2017 compliance deadline.

At the Informal Meeting of Heads of State or Government on 12 February 2015, the members of the European Council emphasised that "*the security of citizens is an immediate necessity. We must better implement and further develop the tools we have. […] We ask that Member States quickly implement the strengthened rules to prevent money laundering and terrorist financing, and that all competent authorities step up action to trace financial flows and to freeze effectively assets used for financing terrorism*."

The Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 28 April 2015 on the European Agenda on Security stated that the Commission "*will also explore the need for and possible benefits of additional measures in the area of terrorism financing, including measures relating to the freezing of terrorist assets under Article 75 TFEU, to illicit trade in cultural goods, to the control of forms of payment such as internet transfers and pre-paid cards, to illicit cash movements and to the strengthening of the cash controls Regulation*."

Finally, the Extraordinary JHA Council of 20 November 2015

"a) invites the Commission to present proposals to strengthen, harmonise and improve the powers of, and the cooperation between Financial Intelligence Units (FIU's), notably through the proper embedment of the FIU.net network for information exchange in Europol, and ensure their fast access to necessary information, in order to enhance the effectiveness and efficiency of the fight against money laundering and terrorist financing in conformity with Financial Action Task Force (FATF) recommendations, to strengthen controls of non-banking payment methods such as electronic/anonymous payments, money remittances, cash-carriers, virtual currencies, transfers of gold or precious metals and pre-paid cards in line with the risk they present and to curb more effectively the illicit trade in cultural goods.

b) is committed to ensure a swift and effective freezing of terrorist assets throughout the Union, whether through autonomous EU decisions or in compliance with UN Security Council Resolutions."

These changes are also reflected in UN Security Council Resolution 2178 that was adopted unanimously on 24 September 2014, which strengthens the UN's commitment to combating foreign terrorist fighters. It specifically notes that Member States must prevent them from travelling or engaging in terrorist acts, which is to be understood in the widest sense, even beyond the wording of the resolution itself. It also underscores that the obligation for Member States to ensure that they have the legal means to bring to justice anyone who is involved in financing or organising terrorist acts also extends to foreign terrorist fighters and their networks.

France considers that new AML/CFT actions at European level are necessary, via the adoption of new legislation to ensure that these new measures have a real, operational impact. In conformity with Council's conclusions, France suggests focusing on the following new areas for action i) bolstering the powers of FIUs in order to improve their cooperative efforts; ii) improving the effectiveness of the European mechanism for freezing terrorist assets at European level; iii) heightening controls and stepping up regulation of payment methods outside of banking circuits; iv) combating illicit trade in cultural goods; v) introduction of bank account registers in the Member States; and vi) launching efforts to set up a European Terrorism Finance Tracking Program (TFTP) to process data from national and international wire transfers (SWIFT system).

The goal of this note is to offer France's contribution to these issues. It lays out possible short-term means for moving forward under current legal conditions and presents elements that justify new legal means to boost the effectiveness of European mechanisms for combating terrorist financing.

1 - Bolstering the powers of FIUs in order to improve their cooperative efforts: critical European harmonisation of FIUs' right of disclosure.

1.1 The right to made additional requests of entities subject to AML/CTF reporting requirements: a distinctive element for the fight against money laundering and terrorist financing

Financial Intelligence Units (FIUs) are tasked with gathering, analysing, supplementing and making use of Suspicious Transaction Reports submitted by entities subject to AML/CFT reporting obligations as well as by other stakeholders, including government offices, supervisory authorities and foreign FIUs.

Analysing and supplementing these reports notably involves additional requests that an FIU may make of reporting entities to have any and all documents and elements relating to a suspicious transaction (bank statements, notarised deeds, company bylaws, accounting documents, invoices, etc.).

These remits and prerogatives, which are set out in Recommendation 29 of the FATF[1], are listed in Articles 32.3 and 33.1b of the Fourth Directive on the prevention of the use of the financial system for the purposes

[1] Recommendation 29: "Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing,

of money laundering or terrorist financing. They play an important role in tracing suspicious financial flows, reconstructing atypical transactions that underpin organised criminal actions, particularly terrorist acts and human trafficking, and as such are critical for effectively combating organised crime both at home and abroad.

1.2. Lack of harmonisation in the exercise of the right of disclosure at European level

Currently, FIUs in certain Member States only have a limited right to obtain additional information. FIUs in certain Member States can only obtain additional information from entities that have already filed STRs, to the exclusion of all others, and they can only, when responding to a request from a foreign FIU, request information from a reporting entity if they have already received an STR concerning the transactions and/or individuals listed in the foreign FIU's request. Moreover, sometimes authorisation from an intermediary authority, such as the courts, is required to request information from a reporting entity.

France considers that:

- the right of FIUs to make additional requests should be specified in the provisions of the Fourth Directive;
- the principle of operational independence and autonomy of FIUs set out in Article 32.2 should be fully implemented by deleting the option that entities may provide the FIU with information "directly or indirectly" (in Article 33.1 b). The intermediation of a third authority undermines and hampers cooperation between FIUs

1.3. Harmonising the European framework related to the exercise of the right of disclosure

It is critical to introduce more specific measures at European level to foster real harmonisation of European practices to ensure an effective AML/CFT mechanism and to bolster international cooperation.

European legislation must clearly stipulate that FIUs may exercise a right of disclosure:

- With respect to a reporting entity even if the entity has not submitted an STR
- At the request of a foreign FIU, including in the absence of an initial STR submitted by a national reporting entity
- Directly: to ensure the quality and completeness of the information submitted, as well as the speed and fluidity of exchanges, that FIUs and reporting entities be able to exchange information directly.

This shift will bring European legislation into line with the consensus achieved at the most recent FATF Plenary Meeting in October 2015 concerning Recommendation 29. The FATF clearly emphasised that an FIU must be able to obtain additional information from all reporting entities, not merely from those that have already submitted an STR. The Task Force also pointed out that obtaining additional information is possible as part of the analysis of a "suspicion". This concept, which goes beyond that of the Suspicious Transaction Report, which was initially called for, allows foreign FIUs to request information from reporting professionals.

---

and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly."

Example: in France, Tracfin can exercise its right of disclosure not only with respect to the entity that submits an STR, but also to all other professionals subject to AML/CFT reporting requirements as set out in Article L.561-2 of the Monetary and Financial Code.

For example, if Bank A sends Tracfin an STR concerning an atypical transaction connected with the account of Mr X, and the Unit checks with the centralised bank account register (FICOBA) and finds that the individual in question also has accounts with Bank B (which heretofore had not filed any STRs concerning Mr X), it can exercise the right of disclosure to obtain additional information not only from Bank A but also from Bank B.

In the same way, it is expressly provided that Tracfin's right of disclosure may be exercised for the purposes of providing information to a foreign FIU. There is no need for Tracfin to be in possession of a prior STR.

For example, if an FIU in another Member State requests information from Tracfin concerning a real estate transaction in France, Tracfin may ask the entity responsible for the sale for information, regardless of the fact that no STR had previously been submitted to Tracfin.

2 - Improving the effectiveness of the European mechanism for freezing terrorist assets

2.1. The shortcomings of the European asset-freezing mechanism

The EU has used asset freezing as a powerful weapon in its foreign policy. Individual measures are systematically a part of its arsenal of restrictive measures put in place as part of sanctions due to situations in certain countries.

Today, "terrorist" assets with links or ties to organisations in third countries (international terrorism) can be frozen autonomously by the EU, under the terms of the Common Foreign and Security Policy (CFSP), pursuant to Council Regulation (EC) No 2580/2001 of 27 December 2001, in line with Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism. This mechanism nevertheless requires that the individual in question must have already been the subject of a decision by a competent authority (launching of an enquiry or conviction), which de facto restricts the scope of the individuals in question.

The EU must quickly put in place a mechanism allowing it to freeze, in a more effective and flexible manner than that stipulated in the current framework (the need for a prior "decision"), assets of individuals who, although being European citizens, are involved in terrorist acts with an international dimension (as is the case with "foreign terrorist fighters" and individuals linked to IS). Moreover, EU Member States should more actively share information about frozen assets of their citizens, so that similar measures could be taken, where necessary, in other countries.

2.2. French proposals

2.2.1. Stepping up implementation of UN assets freeze measures

Implementation of an effective asset freezing mechanism at European level primarily depends on significantly shortening implementation deadlines by the EU of asset freezes decided by the United Nations. Regulations sometimes require weeks to be adopted, although such freezes are intended to be applied "without delay", in line with FATF Recommendation 6. Delays put Member States in breach of their international obligations, and increase the risk that the targeted assets will disappear.

A joint proposal by the EEAS and the Commission is currently being examined by the Member States as part of RELEX / Sanctions efforts, with an eye to adopting measures within 72 hours.

Entities subject to AML/CFT reporting requirements may also be asked, at EU level and throughout the period preceding the entry into force of the freeze measure adopted by the UN, to systematically file STRs concerning transactions by individuals who are the subject of the UN's decision.

2.2.2. Extending asset freezing possibilities at European level

Boosting CFT efforts at European level calls for a renewed mechanism. Currently, the use of Article 215 TFEU (adopting restrictive measures to achieve the objectives of the Common Foreign and Security Policy) appears to be the most appropriate path to bolster the European legal framework. Several means could be explored:

- Adopting a dedicated legal instrument (a new set of sanctions that specifically target IS) that would not only target individuals providing financial support to IS but also the organisation's supply sources
- Amending the Al-Qaida measures (Common Council Position 2002/402/CFSP and Council Regulation (EC) No 881/2002) which to date only repeat the list given in United Nations Security Council resolution 1267, by making autonomous designations possible (European citizens affiliated with IS / foreign terrorist fighters)
- The use of the European asset freezing regime (Council Regulation (EC) No 2580/2001), which nevertheless requires a prior decision by Member States (launching of an enquiry or conviction). As part of this, the possibility of extending a national asset freezing measure to the entire EU should be examined.

In the longer term, the EU could perhaps be given an instrument allowing it to freeze assets of terrorists with no connection to third countries, but whose actions could pose a threat to the entire EU.

2.2.3. Setting up a platform for listing national asset freezes

As national asset-freezing measures are territorial, it is easy for individuals (particularly for those who live near borders) whose assets have been frozen in one Member State to bypass freeze measures and carry out transactions using another Member State's banking system.

Given this situation, France proposes the creation, at European level, of a platform to provide all EU Member States with information about asset freezes instigated by certain Member States. This information shared with all Member States would help reporting entities to step up their vigilance with respect to transactions carried out by individuals whose assets are frozen in another Member State. Entities could inform their FIU about transactions made by such individuals, and even refuse to carry out such transactions.

This freeze information platform could be used as the basis for discussions to extend national freezes EU-wide.

2.2.4. Introducing asset freezes at the request of third countries

United Nations Security Council Resolution 1373 from 2001 requires that countries commit to at least studying asset freeze requests from third countries. This is an international obligation. During the G7 Summit at Schloss Elmau on 8 June 2015, the heads of state and government reaffirmed their commitment to facilitate cross-border freezing requests among G7 countries. At the G20 Summit in Antalya on 16 November 2015, the heads of state and government pledged to enhance cooperation concerning freezing of terrorist assets.

The FATF is currently drafting a handbook of the various national mechanisms for freezing terrorist assets and how to make a formal request to countries. The EU should do the same, to help its members understand the conditions for requesting freezes of the assets of individuals in the various Member States.

Example: France has a national mechanism for freezing the assets of individuals or legal entities who commit, or attempt to commit, terrorist acts, or who facilitate or participate in such acts (Article L.562-1 of the Monetary and Financial Code). The mechanism is aimed at preventing terrorist acts, and their financing in particular. One of the mechanism's goals is to dissuade and discourage individuals who might be associated with terrorist organisations to carry out financial transactions intended to aid or finance such organisations. It is a preventive law enforcement measure, as opposed to a penal measure that is punitive and post-facto. It is independent from, and complementary to, court-ordered measures for freezing the assets of individuals being prosecuted for terrorist acts (in application of the principle of *non bis in idem*).

This administrative measure has already been shown to be effective and dissuasive. Measures to freeze individuals' assets in France – valid for six months – are seldom renewed. Of all freeze measures taken since 2010, only a quarter of them were renewed after six months. This means that it was deemed unnecessary to prolong asset freezes for three-quarters of them, as the risk of terrorist financing was no longer present.

3 - Stepping up verification of payment instruments outside banking circuits: e-money and virtual currencies and strengthening of customs declaration obligations

The recent terrorist attacks in France have shown that some terrorist networks are able to fund themselves clandestinely, often with fairly small amounts. The issue of transaction anonymity, to improve the tracking of suspicious transactions, shall be tackled, not only at national level, but at the EU one for the measures to be fully effective.

The EU regulatory framework needs to be bolstered as follows.

3.1. More effectively regulating and verifying e-money instruments

3.1.1 Regulating more effectively the use of e-money

Electronic money[2] is a resolutely contemporary means of payment which is experiencing rapid and substantial growth owing to the deregulation of the European market following adoption of Directive 2009/110/EC of the European Parliament and of the Commission of 16 September 2009 (Second Electronic Money Directive – 2EMD) which has encouraged competition on the European payments market and fostered the rise of stakeholders with innovative offerings.

But, e-money and, particularly, prepaid cards, that constitute a discreet substitute for cash, could be very widely used by organised crime, migrant traffickers and terrorists. These cards allow for anonymous purchases of items such as airline tickets and weapons. Criminal investigation department officers have already found prepaid cards during searches of the homes of individuals belonging to such networks.

Current EU regulations appear ill-equipped to stop e-money being used for money laundering and terrorist financing.

Directive 2009/110/EC of the European Parliament and of the Commission of 16 September 2009 does regulate the activity of electronic money issuers but fails to comprehensively cover conditions for using this means of payment.

In a similar vein, in the Fourth Anti-Money Laundering Directive (AMLD4)[3], the only provisions on electronic money relate to thresholds and features (cards reloadable or not, able to be used in one or more Member States, maximum storage capacity of the payment instrument or monthly payment transaction limit of EUR 250, etc.) which authorise Member States to allow professionals subject to AML/CFT rules to circumvent certain due diligence measures (such as identification of the customer or beneficial owner).

---

[2] According to EU legislation, e-money includes magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds of an equivalent amount, in consideration of commission and fees. This monetary value must be accepted as a means of payment by a natural or legal person other than the electronic money issuer. See Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

[3] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Whilst the new rules do represent a step forward, they fail to effectively mitigate the inherent risks attached to all forms of electronic money, and to prepaid cards in particular. These cards can hold substantial amounts and their purchase, loading and use are hard to monitor. EU regulations do not require an automatic ID check when purchasing an electronic payment instrument (magnetic stripe or chip cards[4]). Furthermore, there is a real risk of false ID documents being used to obtain prepaid cards. As a rule, the distributors[5] of these cards do not have the means of detecting false ID documents or identity theft. Moreover, they can be loaded anonymously in the sales outlets using cash.

Lastly, the cards are easy to carry and difficult to detect so funds can cross borders discreetly. Prepaid cards look like standard debit/credit cards (even more so when the prepaid card is issued by Visa or Mastercard, etc.) and can be easily hidden from enforcement departments which are unable to ascertain the amount loaded on the card during inspections.

Rapid access to this information is however vital. French Customs recently seized a Panamanian prepaid e-money card in France and was ultimately able to discover that EUR 250,000 was stored on it.

Therefore, the French authorities suggest that the EU adopts the following initiatives:

- Automatic ID check, regardless of the amount loaded, when an individual purchases or reloads an e-money instrument, particularly a prepaid card. Copies of documents provided when the purchase is made or certain information (first names, surname, date and place of birth, etc.) should be kept; a centralised register for this information could be set up.
- Limit the loading and, in particular, the reloading of electronic money instruments by untraceable means of payment (cash, prepaid credits, anonymous e-money)
- Restrict the load capacity of electronic money instruments to a threshold to be decided on
- Track transactions carried out using e-money by operators, issuers, managers and distributors of e-money during all phases of its use (from issue until the money is used up or repaid)

Improving card payment terminals from a technical standpoint should also be looked into. The aim would be to distinguish payments made by prepaid cards from payments made by cards associated with a bank account. In the meantime, the distinction could be visual by adding, for example, a pictogram showing that the card is an e-money instrument[6].

3.1.2 Strengthening oversight and collaboration between EU supervisors for e-money and payment services

EU regulations (directives on payment services and electronic money) allow a payment institution or e-money institution approved in a Member State to carry on its business activity in another Member State under the European Passport, using an agent (payment institutions) or a distributor (e-money institutions). The Fourth Anti-Money Laundering Directive stipulates that the institution applies the AML/CFT rules of the host Member State, under the supervision of that country's competent authority acting "in cooperation

[4] Most cost between EUR 0 and EUR 20.
[5] These prepaid cards are generally sold by tobacconists, local stores and post offices, etc.
6 Article 10.5 of Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

with the competent authority of the home Member State". That said, no details are given as to the form of this cooperation. It also specifies that only "temporary remedial measures" may be taken by the competent authority of the host Member State against European payment or electronic money institutions in the event of serious infringements of AML/CFT rules.

As regards the agents of payment institutions, regulations set out a process under which the competent authority of the home Member State seeks the opinion of the competent authority of the host Member State concerning any suspicion of money laundering or terrorist financing before registering the agent appointed by the foreign institution. In practice, this process is relatively ineffective. In all cases, the competent authority of the home Member State has sole responsibility for the registration/deregistration of agents. Moreover, there are no registration arrangements for e-money distributors.

Lastly, the agents and distributors are individuals or legal entities who/that are not finance sector professionals (shopkeepers, pay phone centres, etc.), and who/that act in the name and on behalf of one or more payment or electronic money institutions, whether European or approved in France.

By its very nature, the system is conducive to suspect customer transactions with a high risk of the agent or distributor aiding and abetting (e.g. presentation of false ID by the customer, registration of false ID document references by the agent, generation of numerous fictitious transactions to get rid of large amounts of cash, disappearance of the agent's business premises once he has registered as an agent, whilst he continues to handle transactions, etc.). In addition, the distinction between transactions carried out on behalf of different organisations and on their own behalf is often blurred.

In light of the foregoing, the French authorities recommend strengthening the legal framework for cooperation on anti-money laundering and combating terrorist financing between the competent European supervisors, and controlling risks relating to carrying on an activity using agents or distributors of payment services or electronic money by:

- rolling out arrangements for e-money distributors aligned, at the very least, with those for agents, as set out in the recently revised Directive on Payment Services: registration of distributors by the competent authority for approvals in the home Member State after running a check on the fit and proper character of the distributor
- regulating the distribution network, using agents or distributors, of a payment or electronic money institution
- obtaining, in a timely manner, and taking account of the opinion of the competent authority of the host Member State before registration of the payment services agent or electronic money distributor by the competent authority of the institution's home Member State
- sending comprehensive information (identity, etc.) on the agents and distributors to the competent authority of the host Member State so that it can provide an opinion on the risks/suspicions in

respect of money laundering and terrorist financing prior to registration by the competent authority of the institution's home Member State

- deregistering payment services agents or electronic money distributors by the competent authority of the home Member State following information sent by the competent authority of the host Member State, especially information from a financial intelligence unit.

The competent authority of the host Member State's responsibility for AML/CFT oversight must be bolstered in practice by acknowledging that it has total authority to impose penalties in these areas, particularly by handing down fines or bans on carrying on a business in its country.

3.2. Regulating and monitoring virtual currencies to improve the transparency of transactions

The nature and operating methods of these currencies, particularly their anonymity and non-traceability when decentralised, make them very difficult to monitor. Many unregulated entities participate in the use of virtual currencies, such as private individuals, groups of people or legal entities. Price and liquidity guarantees are non-existent and their exchange rate is extremely volatile due to their speculative nature. The lack of transparency due to the total anonymity of transactions makes them impossible to monitor for the purposes of countering money laundering and terrorist financing, although some transactions carried out in certain virtual currencies are recorded in a public database.

There is therefore a risk that these currencies will be used for illicit ends, i.e. to finance criminal activities. Some virtual currencies may have been created for this purpose alone; they may be non-traceable due to the use of specific encryption techniques and may not be registered in any transactions database. It is important to note that these currencies may be the underground economy's preferred financing mechanism, particularly the Darknet.

FATF guidance was published in June 2015 to provide these currencies[7] with their first international framework, although the recommendations made are non-binding. In particular, the Task Force recommends that exchange platforms offering to convert virtual currencies into legal currencies should be subject to the rules that govern anti-money laundering and counter-terrorism financing as per FATF standards.

Given the cross-border technologies used, the French authorities recommend subjecting any businesses that convert virtual into legal currencies to anti-money laundering and counter-terrorism financing due diligence rules. Additional measures to improve the regulation of virtual currencies and thus to discourage their use for illicit ends, should be adopted, such as:

- Setting limits for virtual currencies when used as a payment method or when converted into cash.
- Checking customers' identities when converting a virtual currency into a legal currency or when performing a transaction above a certain limit would help combat transaction anonymity and the use of virtual currencies to buy goods or services.

To monitor virtual currencies and combat their use for illicit purposes, France also recommends creating a database to record virtual currency exchange transactions.

[7] *Virtual currencies: Key Definitions and Potential AML-CFT Risks*, June 2015.

3.3 Stepping up border checks on physical transfers of capital by freight, transfers of gold, precious metals and prepaid cards

A large amount of capital is transferred via freight, particularly air freight, escaping Customs declaration requirements which apply only to individuals transferring more than €10,000.

These requirements should be extended to physical transfers of capital by freight, and to transfers of gold, precious metals and prepaid cards. France would like this requirement to be extended to EU borders, which would require changes to Regulation (EC) No 1889/2005 of the European Parliament and of the Council of the European Union of 26 October 2005 on controls of cash entering or leaving the Community.

***Example*:** Given the recognised use of freight and the postal system by criminal organisations and the significant financial flows moving through each, French Customs launched an operation to detect cash movements via normal or express freight or by mail.

Operation Bingo was carried out by the Roissy Fret Customs Directorate in November and December 2014.

It focused on achieving the following goals:

- Obtaining a clear and accurate picture of declared and undeclared capital transfers via normal, express or postal freight.

- Supporting the proposed regulatory changes put forward by the French government to the European Commission, as well as changes at FATF level.

- updating possible money laundering or terrorist financing networks**.**

Regarding the last point, preparatory work found that in 2013, €12 billion in bank notes were declared.

Operation Bingo discovered 90 payment methods were used for a total of €9,244,827 (based on the existing exchange rate), comprising:

- 6 blank cheques with no name entered and an entire cheque book (containing 50 cheques)

- 1 cheque for $44,900

- 83kg of gold and 42.58kg of gold shipped from Togo to Lebanon

- 13 gold ingots weighing 1kg and 8 ingots weighing 500g

- 78 prepaid cards containing an unquantifiable amount of cash

- 2 fund transfer orders of €20,000

- 40 counterfeit €50 banknotes in a postal dispatch from another EU member state. The counterfeit notes apparently came from individuals involved in drug trafficking.

- 651 money orders for a total of $631,470 discovered in an express freight shipment between Togo and the Philippines.

4 - <u>Enhancing the fight against illicit trade in cultural goods</u>

The international community is extremely concerned that terrorist organisations (or related individuals) are involved in the direct or indirect smuggling of cultural goods from archaeological sites, museums, libraries or similar sites to finance their recruitment efforts and to boost their operating resources.

Therefore, France recommends creating a regulatory framework to limit payments by cash or by other non-traceable methods for the purchase of cultural goods to improve monitoring of cross-border transactions in this area.

We should also introduce checks on imports entering the European Union to hamper the transport of goods pillaged from sites located in war zones or illicitly traded objects. This step would enable us to extend existing checks to focus on cultural goods imported from Iraq and Syria.

Currently, EU regulations apply only to the export of cultural goods (Regulation (EC) No 116/2009 of the Council of the European Union of 18 December 2008), with the exception of goods from Iraq and Syria which are checked on import in application of Council Regulation (EC) No 1210/2003 and Council Regulation (EC) No 1332/2013 concerning Iraq and Syria respectively.

Aware of the situation in war zones, European authorities recently examined the possibility of drafting general regulations concerning import checks that would help to combat effectively the illicit trade in cultural goods regardless of the source or origin.

The French authorities support a European-led legislative initiative to create a procedure for performing import checks on cultural goods which would help to bolster existing or planned checks at national level.

Exporting countries must also implement policies requiring export authorisation and clear certificates detailing the origin of these goods.

5 – <u>Creating a national centralised bank account register in each member state</u>

The Council of the European Union 12 February 2015 recommended taking measures to ensure "*that all competent authorities step up action to trace financial flows and to freeze effectively assets used for financing terrorism*".

In France, quick implementation of measures to freeze terrorists' assets is reliant on the existence of the aforementioned bank account register; Tracfin, France's financial intelligence unit, makes extensive use of this register when carrying out investigations and can deal with all requests from its EU counterparts as a result. The register fully safeguards the confidentiality of personal data, as do all automatic data exchanges; both are supervised by CNIL, the independent National Commission for Data Protection and Privacy.

The French authorities consider that the setting up of national centralised bank account registers, which is not required by the 4th Anti-Money Laundering Directive is justified by the current terrorist threat.

To effectively combat terrorist financing, financial intelligence units and supervisory authorities must have access to banking data quickly and in compliance with the confidentiality principle via a centralised bank

account register. Based on a model that already exists in several member states, this register would be a key tool for financial intelligence units and supervisory authorities to effectively carry out investigations and analyses of terrorist financing. It would also pave the way for the introduction of measures to freeze terrorists' assets and promote the exchange of information between member states' supervisory authorities and financial intelligence units.

Without this type of register, it is harder for the authorities to identify which accounts should be frozen; the resources that financial intelligence units have at their disposal to carry out investigations are not entirely optimal, and communication between them could also be improved.

6 – Preparing the groundwork for the introduction of a Terrorist Finance Tracking Program (TFTP) at European level to make use of SWIFT data on international bank transfers

The secure SWIFT (Society for Worldwide Interbank Financial Telecommunications) system is used in over 80% of national, European and international fund transfers worldwide. The system's data is stored on two servers, one located in the US, the other in Europe. US intelligence services (via the Terrorist Financing Tracking Program – TFTP) have been using this data since 2001 either directly (data stored on the US server) or indirectly (data stored on the European server) via a US/EU agreement. European member states do not have direct access to data stored in Europe, particularly data on EU citizens. They can, however, gain access to this data by making a request to the US on the basis of the US/EU agreement.

French FIU (Tracfin)'s experience shows that the conditions for accessing data established by the US are relatively strict, and reaction times slow. Consequently, the right to request access remains largely theoretical (e.g. requests for other information are made in addition to the data requests, etc.). Furthermore, the system cannot be used to process large amounts of data. It is therefore not suitable for the types of investigations that must be carried out today to combat terrorism, as these require very fast response times to uncover the sometimes vast terrorist financing networks that exist.

French authorities are in favour of creating an autonomous European TFTP as a complement to the US Program which would directly use data on EU citizens (and would cooperate with the US TFTP to use US data).

This type of program would equip the EU with a permanent system that could be used to access SWIFT data which is invaluable for investigations carried out by financial intelligence services to identify and track financial flows, a key element in the fight against terrorism.