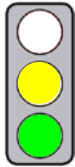


## KEY ISSUES

**Objective of the Regulation:** The traceability of transfers of funds is to be improved in order to prevent and improve the ability to combat money laundering and terrorist financing.

**Parties affected:** Payment service providers, particularly banks.



**Pro:** Combating money laundering and terrorist financing at EU level is necessary because the flow of payments is becoming increasingly transnational in nature.

**Contra:** The regulation cannot be based on the internal market competence (Art. 114 TFEU). Only the flexibility clause can be used (Art. 352 TFEU), which requires unanimity in the Council.

## CONTENT

### Title

**Proposal COM(2013) 44** of 5 February 2013 for a **Regulation** of the European Parliament and of the Council on the **information accompanying transfers of funds**

### Brief Summary

#### ► Aim, definitions and context

- The Regulation is intended to ensure the full traceability of transfers of funds thus facilitating the "prevention, investigation and detection" of money laundering and terrorist financing. (Recital 6, Art. 1)
- The Regulation is intended to implement the recommendations of the Financial Action Transaction Force (FATF) of 2012. The FATF is an international body which develops measures to combat money laundering and terrorist financing.
- The Regulation stipulates the information about the payer and payee that has to be transmitted and stored by the payment service provider when making transfers of funds (Art. 1, Art. 16).
- "Payment service providers" are natural or legal persons who provide the service of transferring funds in a professional capacity, such as banks (Art. 2 (5)).
- "Intermediary payment service providers" are payment service providers who only forward the transfer of funds on behalf of other payment service providers. This is true of correspondent banks that forward transfers of funds to foreign institutions. (Art. 2 (6))
- The Regulation replaces the Transfer of Funds Regulation [(EC) No. 1781/2006]. To accompany this the Commission also proposes a revision of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing [COM(2013) 45].

#### ► Scope

- The regulation applies to transfers of funds between two payment service providers of whom at least one is established in the EU (Art. 3 (1)).
- The regulation does not apply to payment for goods and services using a credit or debit card, mobile telephone or other IT device where the number of the card or appliance is transmitted. This exception does not apply, however, to transfers of funds between two natural persons, such as in the case of a purchase made via an internet auction house. (Art. 3 (2) in conjunction with Art. 2 (10))
- The Regulation also does not apply to (Art. 3 (3))
  - cash withdrawals,
  - payments of taxes, fines or other official levies
  - transfers of funds between payment service providers where these are acting on their own behalf (interbank transactions).

#### ► Information accompanying transfers of funds within the EU

- In the case of transfers of funds within the EU, the payer's payment service provider (hereinafter: paying agent) must transmit to the payee's payment service provider (hereinafter: receiving agent) the following information (Art. 5 (1)):
  - the payer's account number or individual transaction identifier.  
The identifier is a code determined by the payment service provider for each transaction which permits traceability of the transaction back to the payer and payee (Art. 2 (9)).
- At the request of the receiving agent, or an intermediary payment service provider, the paying agent must transmit the following additional information within three days (Art. 5 (2)):
  - the name and account number of the payee,
  - the name of the payer,
  - the payer's address or national identity number or customer identification number or date and place of birth.

► **Information accompanying transfers of funds to countries outside the EU**

- In the case of transfers of funds between a payment service provider established in the EU and a payment service provider established outside the EU, the paying agent must transmit the following information (Art. 4 (1) and (2)):
  - name and account number of the payer and payee, and
  - the payer's address or national identity number or customer identification number or date and place of birth.
- Where no account is used for the transfer of funds, the individual transaction identifier must be transmitted instead of the account number (Art. 4 in conjunction with Art. 2 (9)).
- In the case of transfers of funds to a country outside the EU of up to € 1000 it is only necessary to transmit (Art. 6 (2))
  - the name of the payer and payee and
  - the account number of the payer and payee or the individual transaction identifier.

► **Paying agent's duty to verify**

- The payer's payment service provider must verify the accuracy of the information provided by the payer by way of "documents, data or information obtained from a reliable and independent source" (Art. 4 (3)). The verification and storage of the payer's identity in connection with the opening of the account is sufficient (Art. 4 (4) a)).
- The duty to verify does not apply
  - in the case of a transfer of funds, not made from an account, which is under € 1000, provided it does not appear to be linked to other transfers which together with the transfer in question would exceed € 1000 (Art. 4 (5), and
  - in the case of transfers of funds to countries outside the EU which are under € 1000 provided there is no suspicion of money laundering or terrorist financing (Art. 6 (2)).

► **Duty of receiving agent and intermediary payment service provider to verify**

- The receiving agent and the intermediary payment service provider must
  - verify, by way of "effective procedures" that the information provided is complete (Art. 7 (2), Art.11 (2)),
  - where information is missing, determine, by way of "effective risk-based procedures", whether a transfer of funds should be executed, rejected or suspended (Art. 12 (1), Art. 8 (1)).
- The receiving agent must verify the identity of the payee in the case of a transfer of funds from a country outside the EU (Art. 7 (3) and (4))
  - of over € 1000
  - of up to € 1000 Euro, provided there is a suspicion of money laundering or terrorist financing.
- The receiving agent and the intermediary payment service provider must take steps against payment service providers who are "regularly" in default, ranging from warnings to the rejection of transfer requests and "reconsidering" the business relationship (Art. 8 (2) and Art.12 (2)).
- An intermediary payment service provider may, in the case of payment receipts from countries outside the EU, place technical limitations on information on the payer which passes to the receiving agent; it must then, however, be in a position to inform the receiving agent of the missing information by other means (Art. 14 (3)). On request, the intermediary payment service provider must provide this information within three working days (Art. 14 (4)).

► **Record-keeping and cooperation obligations of the payment service provider**

- A payment service provider must respond to questions from the responsible authorities concerning the information without delay (Art. 15).
- A payment service provider must keep records of the information for five years. An intermediary payment service provider must only keep a record of the information if it has withheld the information from the receiving agent. Member States may extend the maximum retention period to a maximum of ten years. (Art. 16)

► **Sanctions**

- Member States lay down the measures and sanctions applicable to breaches of this Regulation (Art. 17 (1)).
- A breach of the Regulation includes (Art. 18 (1))
  - failure to provide the information,
  - breach of record-keeping obligations,
  - failure to put in place effective risk-based policies and procedures.
- Measures and sanctions are, for example, a public statement of the breach, withdrawal of authorisation and fines. The latter may amount to € 5 million in the case of a natural person and, in the case of a legal person, up to 10% of annual turnover. (Art. 18 (2))

## Main Changes to the Status Quo

- Previously, the paying agent only had to transmit information on the payer to the receiving agent.
- Previously, transfers of funds by way of credit and debit cards, mobile phones and IT devices between natural persons did not fall within the scope of the Regulation.
- Previously, the information on the payer and payee, in the case of transfers of funds to a country outside the EU, always had to be checked.

- ▶ Previously, the identity of the payee in the case of a transfer of funds into the EU from a country outside the EU did not always have to be checked.
- ▶ Previously, the procedures to be followed in the case of missing information were not risk-based but rule-based.
- ▶ Previously, intermediary payment service providers did not have to check that information transmitted was complete.
- ▶ Previously, there was no explicit maximum retention period for information.

### Statement on Subsidiarity by the Commission

The Commission fears that non-coordinated action by Member States will impact on the "smooth functioning" of the EU payment system.

### Policy Context

Previously, the Transfer of Funds Regulation [(EC) No. 1781/2006] governed the information accompanying transfers of funds. In parallel, the "third money laundering Directive" (2005/60/EC), which aims to prevent the use of the financial system for money laundering and terrorist financing, is being revised [COM (2013) 45]. Other legal acts to combat money laundering and terrorist financing are the Regulation on controls of cash entering or leaving the EU [(EC) No. 1889/2005], the payment service Directive on payment services in the internal market (2007/64/EC) and the Regulation on specific restrictive measures to combat terrorism [(EC) No. 2580/2001].

### Legislative Procedure

5 February 2013 Adoption by the Commission  
 Open Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

### Options for Influencing the Political Process

Leading Directorate General:	DG Internal Market
Leading Committee of the EP:	Civil Liberties, Justice and Home Affairs; Rapporteur Timothy Kirkhope (ECR Group, UK)
Leading Federal Ministry:	Ministry of Finance
Leading Committee of the BT:	Finance
Decision mode in the Council:	Qualified majority (Adoption by a majority of the Member States and with 255 of 345 votes; Germany: 29 votes)

### Formalities

Legal competence:	Art. 114 TFEU
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Legislative procedure:	Art. 294 TFEU (ordinary legislative procedure)

## ASSESSMENT

### Economic Impact Assessment

**Money laundering and the financing of terrorism are damaging to the citizens and states of the EU** both directly and, by undermining confidence in the Rule of Law, also indirectly. **Efforts to combat them at international level** by the FATF and the EU **are factually necessary because the flow of payments is becoming increasingly transnational in nature**. International cooperation within the framework of the FATF and the global implementation of its recommendations prevents regulatory arbitrage and the distortion of competition.

The extension of the scope to cover transfers of funds between natural persons is logical considering the rapid technological changes in procedures for transferring funds. It reduces, on the one hand, the ability of money launderers and terrorists to avoid detection by using less well-regulated payment procedures. On the other hand, the competitive neutrality of the various payment procedures is increased.

**The now compulsory transmission of information on the payee of a transfer of funds facilitates the traceability of transfers of funds** and thus the judicial processing of cases of money laundering and terrorist financing. For the same reason, it is appropriate that intermediary payment service providers have to check the completeness of the information on the payer and payee and, where required, keep a record of it. This enables errors in the transmission of information - particularly where several payment service providers are involved - to be found more easily and investigation procedures are less time consuming. This in turn improves the traceability of transfers of funds.

The transfer from rule-based to risk-based procedures, for determining how to proceed in the case of missing information, is also appropriate: **By individually assessing and weighting risks, the payment service provider can explicitly steer resources to areas with a high risk of money laundering**. They can thus concentrate more on country-specific risks and those which relate to their own business activity. Risk-based procedures can also be adapted more quickly than rule-based ones to take in new risks arising as a result of future technological developments, for example.

It is not clear why the Commission has sometimes used new terminology rather than reverting to existing legal acts such as the payment services Directive (Directive 2007/64/EC) which specifies which service providers are considered to be payment service providers (e.g. E-Banks). This leads to inconsistencies and thus to legal uncertainty and should be rectified.

## Legal Assessment

### Legislative competence

**The Regulation cannot be based on the internal market competence (Art. 114 TFEU)**, which empowers the EU to harmonise national provisions in the interests of the internal market, **because it is expressly aimed at the "prevention, detection and investigation of money laundering and terrorist financing"** (Art. 1). The focus is therefore on possibilities for improving prosecution rather than on the functioning of the internal market. It is nevertheless to be expected that the ECJ will approve the internal market competence as the legal basis [cf. ECJ, Case C-301/06 of 10 February 2009 on the Directive on the retention of data (2006/24/EC)].

The legal basis for police cooperation (Art. 87 TFEU) does not apply either because it requires cooperation between authorities.

**The only remaining possibility as legal basis for competence is the flexibility clause (Art. 352 TFEU)**. This allows the EU to take measures in areas of policy covered by the EU Treaties in order to achieve one of the objectives of the Treaties if the Treaties have not provided the necessary powers. Police and judicial cooperation in criminal matters is an area of policy covered by the Treaties (Art. 82 et seq. TFEU), the creation of an "area of freedom, security and justice" an appropriate objective (Art. 3 (2) TEU). Nowhere else do the Treaties empower the EU to require private bodies to collect and store information (see above). The flexibility clause requires unanimity in the Council.

### Subsidiarity

The flow of payments is becoming increasingly transnational so it makes sense to have regulations at EU level.

### Proportionality

The choice of Regulation as the form of legislation is appropriate. The FATF recommendations contain hardly any scope for discretion when it comes to implementation. In the interests of a single payment area within the EU, the few alternatives offered by the FATF should also be uniformly regulated EU wide.

### Compatibility with EU law

The groundless storage of the information required to accompany transfers of funds interferes with the right to protection of personal data [Art. 8 Charter of Fundamental Rights of the EU (CFREU), Art. 16 TFEU]. This interference is justified however. Both the "prevention and combating of criminality" as well as the functioning of the internal market are, as Union objectives (Art. 3 TEU), permitted grounds for limitation. In particular, the Regulation expressly serves only to combat money laundering and terrorist financing.

### Compatibility with German law

The groundless storage of the information required to accompany transfers of funds does interfere with the right to informational self-determination [Art. 2 (1) in conjunction with Art. 1 (1) Basic Law (GG, German Constitution)] Due to concerns about data protection law, the Federal Constitutional Court also considered the implementation law on the Directive on the retention of data (2006/24/EC) to be in breach of the - as compared with the right to informational self-determination - more specific fundamental right of secrecy of telecommunications (Art. 10 GG) (BVerfG, 1 BvR 256/08 of 2 March 2010). It stated that, in order to conform with the principle of proportionality, inter alia, a limitation on the purposes for which the data is to be used was required. The Regulation on information accompanying transfers of funds, however, provides that data accompanying transfers of funds can only be used to combat money laundering and terrorist financing, thus this requirement has been met.

In other respects, the Federal Constitutional Court rejects the need for an assessment of secondary EU law for conformity with fundamental rights under the Basic Law provided there is effective protection at EU level which essentially corresponds to that provided under German law (BVerfG, 2 BvR 197/83 of 22 October 1986, „Solange II“ Case).

## Conclusion

Money laundering and the financing of terrorism are damaging to the citizens and states of the EU; efforts to combat them at international level are factually necessary because the flow of payments is becoming increasingly transnational in nature. The compulsory transmission of information on the payee of a transfer of funds facilitates the traceability of transfers of funds. By individually assessing and weighting risks, the payment service provider can explicitly steer resources to areas with a high risk of money laundering. The Regulation cannot be based on the internal market competence (Art. 114 TFEU), because it is expressly aimed at the "prevention, detection and investigation of money laundering and terrorist financing". The only remaining possibility is the flexibility clause (Art. 352 TFEU) which requires unanimity in the Council.