Deutsche Bank
Global Transaction Banking

EU Funds Transfer Regulation 2015:

A regional regulation with a global impact

May 2017

Contents

Introduction

While the EU Funds Transfer Regulation 2015 (Regulation (EU) 2015/847), hereafter FTR 2015,[1] updates and extends the existing requirements of FTR 2006,[2] the changes and challenges it brings are more significant than meet the eye.

With its requirements becoming applicable on June 26, 2017, there are a number of implementation hurdles ahead. One such stumbling block is the significant room for interpretation that currently exists within FTR 2015, with several aspects of the regulation prompting more questions than answers as it does not set out in detail what Payment Service Providers (PSPs) should do to comply.

The issue is, if the requirements are unclear or open to interpretation, disruptions to payment flows or unintended breaches of the regulation may likely occur, as well as a fragmentation to the regulatory landscape. This may not only lead to a negative impact on individual banks, but also on senior managers who are personally liable for the organisation's controls. Above all, a lack of clarity and focus could also harm the effectiveness of the regulation in achieving its objective: to increase the effectiveness of the fight against money laundering and terrorist financing.

As such, a common understanding among financial institutions and regulators of the scope and requirements of FTR 2015 will be necessary to help address industry concerns around anti-money laundering and counter-terrorist financing – and to prevent unnecessary payment disruption post-June 26.

At the beginning of April 2017, the European Supervisory Authorities (ESAs) issued draft guidelines relating to FTR 2015 and launched a public consultation.[3] The draft guidelines, while intended to promote the development of a common understanding to ensure a consistent application of EU law, do not, however, aim to achieve maximum harmonisation of PSPs' approaches to complying with FTR 2015.

We hope that this whitepaper will contribute towards a common understanding, while pinpointing key areas where further clarification would be welcomed.

Should you wish to discuss any of the topics raised in more detail, don't hesitate to contact your local Deutsche Bank representative.

Significant room for interpretation currently exists within FTR 2015

Christian Westerhaus
Head of Product & Strategy, Institutional Cash Management, Deutsche Bank

[1]Source: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R0847
[2]Source: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006R1781
[3]Source: http://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-to-prevent-transfers-of-funds-can-be-abused-for-ml-and-tf/-/regulatory-activity/consultation-paper

Section One: Reinforcing payments' regulatory foundations

In recent years, governments and regulators worldwide have sought to update and strengthen anti-money laundering (AML) and counter-terrorist financing (CTF) regulation. FTR 2015 plays an important role in this regulatory drive.

The purpose of FTR 2015, which becomes applicable on June 26, 2017, is to ensure traceability of payment transactions – a powerful tool in the prevention, detection and investigation of money laundering and terrorist financing.

The regulation updates and extends the existing requirements of its predecessor, FTR 2006, and aims to give effect to updated international AML/CTF standards set by the Financial Action Task Force (FATF), namely Recommendation 16 on wire transfers.

As such, FTR 2015 broadens the regulatory requirements around the information relating to payers and payees that must accompany a transfer of funds, sent or received in any currency, when either the payer's or payee's Payment Service Provider (PSP), or an intermediary PSP, is established in the European Union (EU) or the European Economic Area (EEA).

It is worth noting that the effective date of FTR 2015 has been aligned with that of the EU's fourth Anti Money Laundering Directive (AMLD IV) to help ensure the smooth introduction of the new AML/

A co-ordinated approach: is FATF enough?

Established in 1989, FATF is an inter-governmental body whose mandate is to set standards and promote the effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF Recommendations, updated in February 2012, set out a comprehensive and consistent framework for achieving this. These Recommendations are, however, non-binding since "countries have diverse legal, administrative and operational frameworks and different financial systems and so cannot all take identical measures to counter these threats".[4]

Often, this means that these standards are neither immediately nor fully transposed into the local laws of FATF member states, or in some cases they are transposed in deviation to FATF recommendations.

Therefore, in many countries, similar – though not identical – standards apply. In turn, this creates an uneven terrain of AML/CTF measures upon which regulations such as FTR 2015 attempt to build their foundations.

At Deutsche Bank, we believe that a comprehensive AML/CTF regulatory framework is essential for enabling financial institutions to make a meaningful contribution to the prevention of illegal activities. Indeed, failure to achieve this could lead to significant societal repercussions.

[4]Source: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

CTF framework within the EU. The two initiatives are not interdependent; rather, they are part of a wider effort by the EU to crack down on global illicit financial flows.

The sheer scale of money laundering alone is a significant incentive for governments and regulators to intensify their fight against it. According to estimates from the United Nations Office on Drugs and Crime (UNODC), annual global money laundering flows account for 2%-5% of global GDP, equivalent to USD 800 billion-USD 2 trillion.[5] This activity can significantly undermine the integrity and stability of the financial sector, as well as the broader economy and society as a whole.

Keeping one step ahead of illicit activities is, however, becoming more of a challenge since modern technology gives rise to increasingly sophisticated methods of money laundering. In addition, the interconnectedness of today's global economy means that more cross-border transactions are taking place, and these can be harder to monitor end-to-end for suspicious activity. This is precisely why co-ordinated regulatory action on AML/CTF is so important.

FTR 2015 broadens the regulatory requirements around the information relating to payers and payees

[5]Source: http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/anti-money-laundering.html

Section Two: Understanding the scope and requirements of FTR 2015

Since FTR 2015 is the result of repealing and updating FTR 2006, the updated regulation does not change existing principles per se, but extends the currently applicable requirements. The incoming changes therefore represent an evolution of existing AML and CTF measures, rather than a revolution.

Nevertheless, its impact should not be underestimated. Most notably, FTR 2015:

1. Imposes additional requirements on intermediary PSPs to implement effective procedures to detect whether regulatory required information is transmitted with a transfer of funds.
2. Requires transmission of payee information.
3. Sets higher (qualitative) standards on PSPs to implement effective procedures to detect missing/ insufficient information.

The transmission of payee details (name and account) is already a market standard (for SEPA Credit Transfers, transmitting the payee's name and account number is even mandatory pursuant to EU Reg. 2012/260). Nevertheless, making this a FTR 2015 requirement constitutes an important change. By making transmission of information on the payee mandatory, FTR's "Detection Requirements" now also relate to the payee information. Accordingly, transfers of funds must be checked for this information, and, if not sufficiently transmitted, the receiving PSP must consider this when deciding whether to execute, suspend or reject the transfer. In addition, insufficient transmission constitutes a "failure" that, if occurring repeatedly, might trigger measures against that PSP and might have to be reported to the respective regulatory authorities.

Who must comply?

As outlined, FTR 2015 applies to a transfer of funds, in any currency, sent or received by a PSP, or an intermediary PSP, established in the EU or any of the three additional countries of the EEA (Iceland, Liechtenstein, and Norway).

Impact on PSU

Importantly, FTR 2015 does not impose any obligations on payment service users directly. It is the PSPs that are responsible and must ensure that FTR 2015 requirements are complied with.

Impact on PSPs outside the EEA

Despite being a regional regulation, all financial institutions – regardless of location – must be aware of its global repercussions. Transfers sent from outside the EEA to a PSP established in the EEA will have to be checked by that PSP for transmission of certain information. While a PSP established outside the EEA cannot breach FTR 2015 requirements when sending transfers, it should still consider sending all the information required under FTR 2015 when sending a transfer to the EEA. This will, of course, only be possible to the extent permissible by the PSP's respective local law, in particular, local data protection laws.

Other regulatory obligations

Within the EEA, the FTR 2015 requirements apply without prejudice to any other regulatory obligations. Regulation (EU) 260/2012, which lays down additional information requirements for credit transfers and direct debits made in euro, must therefore (continue to) be observed as well. Similarly, more rigid control requirements deriving from other EEA and local legislations, such as anti-financial-crime regulations, are not altered by FTR 2015.

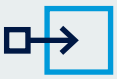
FTR 2015 geography

FTR 2015 applies to all countries of the EU and the three additional countries of the EEA. It may also apply to countries/territories sharing a monetary union with an EU member state, such as Monaco and the Channel Islands – subject to an application and successful approval process. Transfers of funds between these countries/territories and the relevant EU member state will then be treated as transfers of funds within this particular EU member state.

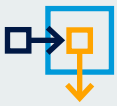
In scope are all transfers of funds:

Within the EEA

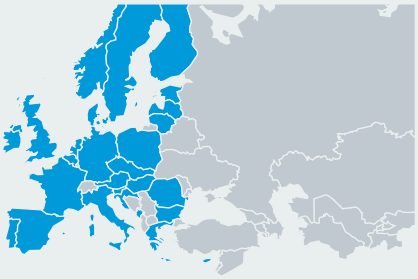
From within the EEA to outside the EEA



From outside the EEA into the EEA



From outside the EEA via an intermediary PSP within the EEA to a country outside the EEA



For FTR 2015 to apply, only one PSP in the payment chain has to be established in the EEA.

'Established' refers to the account maintaining unit, so it is not important where the entity is registered.

Therefore:

A branch that is established outside of the EEA is not in scope of FTR 2015 requirements

Where an entity is established outside the EEA and its branch is established within the EEA, FTR 2015 requirements apply to such branch (however, not to the entity established outside the EEA)

Information requirements

Under FTR 2015, the payer's PSP must ensure that certain information accompanies a transfer of funds. Similarly, intermediary PSPs are required to ensure that all information on the payer and payee that is received must be retained with the transfer of funds.

The information requirements differ depending on the location of the PSPs involved in the transaction chain, and the amount of the payment transaction:

1. Minimum/maximum information requirements

In principle, the following information must be transmitted with a transfer of funds pursuant to FTR 2015:

- Name of the payer
- Payer's account number
- Payer's address
- Name of the payee
- Payee's account number

Exceptions

However, there are some exceptions where less or other information may be transmitted instead:

- Depending on the scenario, less information can be transmitted (see table overleaf).
- Instead of the payer's address, transmission of an official personal document number, customer identification number, or date and place of birth would be allowed as well.
- Where a transfer is not made from or to a payment account, a "unique transaction identifier" which permits traceability back to the payer/payee must be transmitted instead of the respective (non-existent) payment account number.
- Where individual transfers of a single payer are batched together and the payees' PSPs are established outside the EEA, the individual transfers bundled in the batch file do not have to be accompanied by information on the payer provided that the batch file contains the information on the payer and that the individual transfers carry the payment account number of the payer (or a unique transaction identifier respectively).

Scenarios

From the perspective of the payer's PSP (established in the EEA), the following information must – as a minimum – be sent with a transfer of funds under FTR 2015:

	Payer's Name	Payer's Account Number	Payer's Address	Payee's Name	Payee's Account Number
To a Payee PSP established in the EEA		Y			Y
To a Payee PSP established outside the EEA above EUR 1000 (or "linked" above EUR 1000)	Y	Y	Y	Y	Y
To a Payee PSP established outside the EEA below EUR 1000 (and not "linked" above EUR 1000)	Y	Y		Y	Y
To a Payee PSP established in the EEA but with reason to believe that the intermediary PSP is established outside the EEA	Y	Y	(Y) depending on amount	Y	Y

Note: in case of transactions sent to/via a non-EEA country transmission of full information should always be considered (as this might be required pursuant to the respective non-EEA laws and regulations the receiving PSP has to observe).

Note the exceptions listed on page 7.

2. Where and how information should be transmitted

FTR 2015 stipulates that the regulatory required information on the payer and the payee is transmitted end-to-end with the transfer. There are a number of aspects to consider around this, including:

a) Designated field formatting

FTR 2015 does not (directly) impose specific obligations on the payer's PSP or intermediary PSPs on how regulatory required information in relation to the payer or payee must be transmitted.

However, both the intermediary PSPs and the payee's PSP respectively must implement procedures to detect whether the information has been transmitted in a specific way. In particular, they must detect whether the regulatory required information is provided in the designated data fields as required by the conventions of the respective payment message scheme.

Therefore, if a scheme stipulates that a specific field is to be used for the payer's name, then this field must be used and not any other. Regulatory required information in relation to the payer or payee that is not provided in the designated data fields (as required by the conventions of the respective scheme) is – for the purpose of FTR 2015 – not sufficiently provided by the sending PSP.

b) Switching into payment systems with technical limitations

Intermediary PSPs established in the EEA must ensure that all the information received on the payer and payee that accompanies a transfer of funds must be retained with the transfer. FTR 2006 has in essence the same requirement. However, FTR 2006 allows intermediary PSPs to use payment schemes with technical limitations under specific circumstances, even if – as a result – information on the payer is not then transmitted with the payment transaction. FTR 2015, however, no longer allows for such optionality (although FATF 16 still does).

This change in law is most relevant in cases where a cross-border transfer is switched into a local clearing scheme. For example, local clearing schemes in the EEA (currently) require that local IBANs are transmitted in the designated fields. As such, for cross-border transfers, the non-local payer's account number cannot be transmitted in the designated "payer's account number" field.

Although today's market practice is that intermediary PSPs switch cross-border transfers into local clearing by substituting the non-local payer's account number in the respective designated field with a local intermediary PSP's account number, such practice cannot continue under FTR 2015.

3. Assurance of accuracy of payer information

As explained, the payer's PSP must ensure that the regulatory required information is transmitted with the transfer of funds.

- Regarding information on the payee, the payer must provide this information in the payment instruction to enable the payer's PSP to transmit the required information with the transfer.
- Regarding information on the payer, however, the payer's PSP must not only ensure that information is as such transmitted, the payer's PSP must also ensure (in other words, "verify") that this information is accurate (at least if the transaction amount exceeds EUR 1000). To comply with this requirement, a payer's PSP may rely on its existing KYC information on the payer. Accordingly, the payer's PSP can populate the regulatory required information from the payer's static KYC information to ensure its compliance with this requirement.

4. Detection and verification requirements

a) Detection

Under FTR 2015, intermediary and payee PSPs must put in place effective procedures to detect whether the designated payment message data fields in relation to the payer/payee are filled using the characters or inputs admissible in accordance with the conventions of the respective system.

Pursuant to the ESAs' draft guidelines, the monitoring of transfers of funds in relation to these requirements should be in real-time. However, a PSP may assume that it complies with this requirement (already) if the system's validation rules meets certain requirements, in particular automatically prevent the sending/receiving of payments with inadmissible characters or inputs.

Furthermore, intermediary and payee PSPs must put in place effective procedures to detect whether the required (complete) information on the payer/payee has been transmitted (see table below for minimum information requirements).

Pursuant to the ESAs' draft guidelines, the procedures may consist of a combination of ex-post (including random and targeted sampling) and real-time monitoring (for high-risk transfers, as defined by the ESA).

In essence, these procedures require a "meaningful character check" as per market practice today. Obviously, meaningless information must be treated as though it was missing. Whereas these requirements already existed in relation to the payee's PSP and payer information, these requirements are now also extended to intermediary PSPs and payee information.

b) Verification (payee's PSP only)

In addition to the checks above, the payee's PSP must, under certain circumstances, verify the information received on the payee. The payee's PSP may, in this context, rely on its KYC process and respective proper identification of the payee. This requirement is an inverse of the verification requirement for the payer's PSP.

Nevertheless, it is unclear whether in this context – or at least in certain scenarios – a "name-number-check" must be conducted (see Section Three for further details).

These procedures require a "meaningful character check" as per market practice today

Minimum information requirements: from an intermediary PSP (established in the EEA) perspective

	Payer's Name	Payer's Account Number	Payer's Address	Payee's Name	Payee's Account Number
From a Payer PSP established in the EEA to a Payee PSP established in the EEA		Y			Y
From a Payer PSP established in the EEA to a Payee PSP established outside the EEA above EUR 1000 (or "linked" above EUR 1000)	Y	Y	Y	Y	Y
From a Payer PSP established in the EEA to Payee PSP established outside the EEA below EUR 1000 (and not "linked" above EUR 1000)	Y	Y		Y	Y
From a Payer PSP established outside the EEA	Y	Y	Y	Y	Y

Note the exceptions listed on page 7.

Minimum information requirements: from the payee's PSP (established in the EEA) perspective

	Payer's Name	Payer's Account Number	Payer's Address	Payee's Name	Payee's Account Number
From a Payer PSP established in the EEA		Y			Y
From a Payer PSP established outside the EEA	Y	Y	Y	Y	Y

Note: For the payee's PSP it is irrelevant whether an intermediary PSP involved in the transactions chain is located inside or outside the EEA. The location of the payer's PSP only matters from the perspective of the payee's PSP.

Note the exceptions listed on page 7.

5. Handling of insufficient information

The overall regulatory aim of FTR 2015 is to ensure full traceability of payment transactions as this can be a particularly important tool in the prevention, detection and investigation of money laundering and terrorist financing. The information requirements provide for a comprehensive system in this regard.

This includes the obligation imposed on PSPs to decide, using effective risk-based procedures, whether to execute, suspend or reject a transfer of funds, to request missing information (in instances where the transfer is not rejected) and, in case of repeated failures of other PSPs, to inform competent authorities hereof, to issue warnings including setting of deadlines, and, in severe case, reject of all future payment transactions from that PSP up to even terminating the entire business relationship. In addition, missing or incomplete information must be considered as a factor for Suspicious Activities Reporting.

The following steps should help PSPs in handling instances of insufficient information:

a) Make a decision on execution and sending of request for information

Intermediary PSPs and the payee's

PSPs must implement effective risk-based procedures to determine whether to execute, reject or suspend a payment transaction that is lacking the regulatory required (complete) information on the payer or the payee.

Although missing information can sometimes be cause for suspicion, it does not in itself point to money laundering or terrorist financing. As such, neither an in-principle rejection of all transfers missing information nor a suspension of such payments until the missing information can be obtained from the payer's PSP is required from a risk-based perspective.

Pursuant to the ESAs' draft guidelines, PSPs should consider the money-laundering/terrorist financing risks associated with the individual transfer (in particular whether the type of information missing gives rise to concern, the transfer is from a high risk country).

Where a PSP decides not to reject a transfer that is missing regulatory required information it must send a request for the missing information. The same applies in instances where a PSP detects ex-post that information is missing. The payer's PSP, established in the EEA, is required to make available the regulatory required information within three working days of receiving the request for information (the information that must, at least, be made available depends on the location of the PSPs involved in the transaction chain and the transaction amount).

Pursuant to the ESAs' draft guidelines, PSPs established outside the EEA should be expected to reply to requests for information within five working days.

It is worth noting that even in instances where the minimum regulatory required information is not missing, the payee's PSP or intermediary PSP can still request additional information.

b) Repeated failures: appropriate follow-up actions

In instances where another PSP "repeatedly" fails to provide the required information, the receiving PSP must react and take the following so-called "additional steps":

1. Start with the issuance of warnings including setting of deadlines
2. And, should the PSP not adjust its behaviour even after warnings and deadlines:
   - Future transfers involving this PSP must be rejected
   - Or – at worst – the entire business relationship has to be terminated

In addition, the respective local competent authorities responsible for monitoring compliance with anti-money laundering and counter-terrorist financing provision must be informed if a PSP repeatedly fails to provide the required information, including the additional steps taken above.

Repeated failures: two challenges to overcome

1. When is a PSP "repeatedly" failing to provide the required information?

   FTR 2015 provides no guidance as to when failures must be considered "repeated". Pursuant to the ESAs' draft guidelines, PSPs may decide to treat other PSPs as repeatedly failing for different reasons, which may include either/or a combination of quantitative and qualitative criteria.

2. When and how should regulators be informed?

   FTR 2015 also provides no guidance on the reporting cycle to local regulators, or on the level of details that must be provided. Pursuant to the ESAs' draft guidelines, regulators must be informed on repeated failures within one month, or earlier, if required by local law.

See Section Three of this whitepaper for further details on these issues.

—

Separate from the decision whether to execute, suspend or reject a transaction missing or incomplete information must be considered as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it has to be reported to the EU Financial Intelligence Units (pursuant to AMLD IV).

—

In addition, national competent authorities responsible for monitoring compliance with AML/CTF provisions will, in instances of ambiguity or a lack of clear guidance, impose deviating requirements and expectations on PSPs – resulting in a fragmented regulatory landscape.

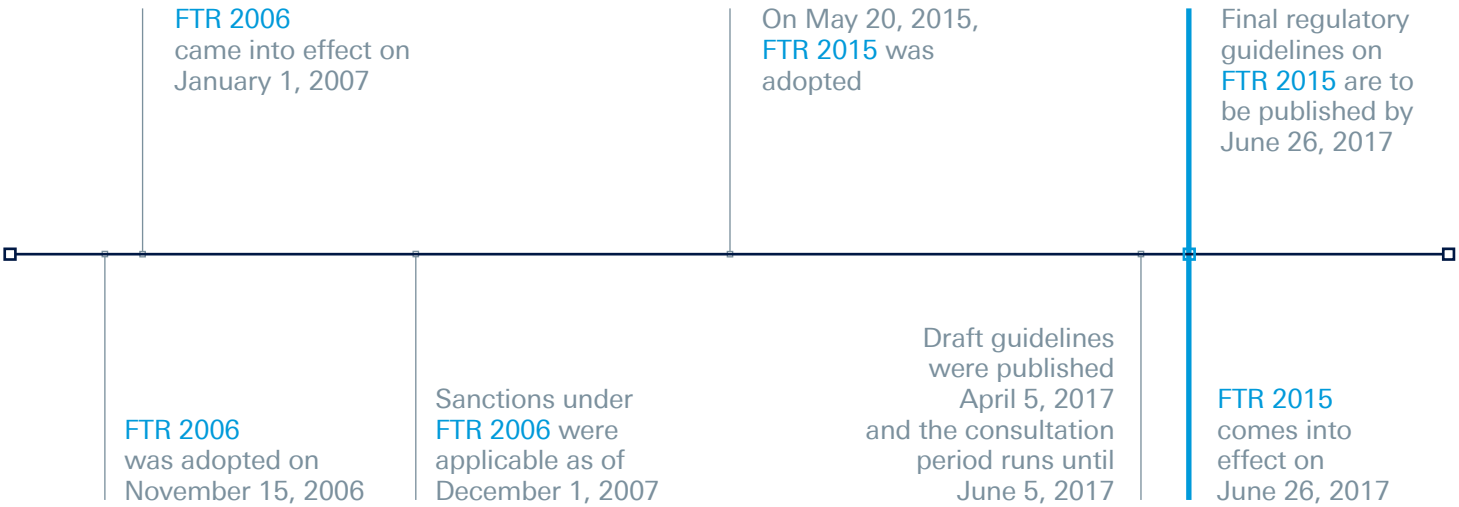
While the approach taken by the ESAs' in the draft guidelines provides PSPs some flexibility to accommodate for different risk scenarios, it also carries the risk of a fragmented regulatory landscape and disruptions in payment flows. Deutsche Bank would therefore welcome further dialogue during the consultancy phase to provide clarity with respect to key areas and topics.

An impact on the entire industry

To be able to efficiently fight money laundering and the financing of terrorism, Deutsche Bank believes that a common understanding, as well as a consistent implementation/application of FTR 2015 requirements by PSPs and regulators, is vital.

Even seemingly small definitional ambiguities can have significant impacts on how different banks interpret FTR 2015 and, therefore, how they build their processes around it. This could impact the entire banking industry.

Timeline



Section Three: Overcoming the barriers to implementation

As explained, FTR 2015 leaves significant room for interpretation as it does not set out in detail what PSPs must do to comply.

While the ESAs' draft guidelines provide further clarity, they do not, however, aim to achieve maximum harmonisation of PSPs' approaches to complying with FTR 2015. Furthermore, the draft guidelines are limited in scope on measures to comply with Art 7, 8, 11 and 12 (detection requirements and handling of transfers with missing information) and to a limited extent Art 9 and 13 (suspicious activities assessment and reporting). Accordingly, questions remain, such as:

1. What constitutes a "repeated failure"?

   As discussed in Section Two, when another PSP repeatedly fails to supply the required information, the receiving PSP must react and take (successive) so-called "additional steps" in relation to the PSP and inform competent authorities on the repeated failure and the additional steps taken.

   As aforementioned, while FTR 2015 provides no guidance as to when failures must be considered "repeated", pursuant to the ESAs' draft guidelines, PSPs may decide to treat other PSPs as repeatedly failing for different reasons, which may include either/or a combination of quantitative and qualitative criteria.

   As the potential consequences attached to repeated failures are significant, and since the respective regulatory reporting is not optional (but mandatory), a consistent understanding of the "trigger" is required both by PSPs and the respective competent authorities. The final guidelines should aim for maximum harmonisation in this regard and provide detailed requirements.

2. What constitutes a "linked" transaction?

   In certain scenarios to benefit from exemptions, or when determining whether required information has sufficiently been transmitted with a transfer, PSPs must be able to detect whether transactions are linked.

   Whereas FTR 2015 does not provide any guidance, the ESAs' draft guidelines define at least those transactions as linked that are being sent:

   - From the same payments account or the same payer to the same payee; and
   - Within a short timeframe, for example within six months.

   In light of the suggested timeframe of six months it is doubtful whether a payer's PSP would make use of the exemption, as it would require significant IT capabilities (likely outweighing any potential gains). Whereas a payer's PSP can choose to not make use of the exemptions, intermediary and payee PSPs do not share this liberty.

   For example, in the case of a transaction where the payer's PSP is established inside the EEA and the payee's PSP is established outside the EEA, the payer's PSP may send transactions not exceeding EUR 1000 that do not appear to be linked to other payment transactions which, together with the payment transaction in question, exceed EUR 1000 without the payer's address.

Accordingly, an intermediary PSP that is established in the EEA must check, in these cases, whether transactions that are below EUR 1000 and that have been sent by the payer's PSP without the payer's address are linked to other transactions to determine whether required information is missing.

If intermediary PSPs must consider transactions in a timeframe of six months as potentially "linked", one conceivable reaction might be that intermediary PSPs will, as a matter of principle, not accept transactions without full information in this scenario.

It remains to be seen whether the definition of linked transactions will be further developed during the consultation phase.

3. Is a name-number-check required?

Pursuant to Art 7 of FTR 2015, the payee's PSP is required to (i) detect whether regulatory required information is transmitted in the designated fields and (ii) verify the accuracy of the information received on the payee in certain scenarios. It is unclear, whether as a result of this verification requirement, a name-number-check has to be conducted in certain scenarios or under certain conditions.

One interpretation is that, in instances where the payment is to be credited to a payee's payment account (and the payee's PSP has no reasonable grounds for suspecting money laundering or terrorist financing) pursuant to Art 7 (1) to (4) FTR 2015:

- For all intra-EEA payments, a name-number-check is not required (Art 7 (3) in combination with para (2) (a). However;
- A name-number-check would be required (unless Art 7 (5) applies) for payments exceeding EUR 1000 (or that are "linked" above EUR 1000) where the PSP of the payer is established outside the EEA (Art 7 (3) in combination with para (2) (b)).

However, pursuant to Art 7 (5) such a verification check is, in principle, not required if the identity of the payee has already sufficiently been verified (e.g. in a proper KYC check during the onboarding process).

It is unclear, based on which information contained in a payment message if the payee's PSP should determine whether the preconditions are met for Art 7 (5) to apply, i.e. determination if the payee's identity is known ("verified"):

- Either based on the transmitted account number (as a result, whenever the transmitted account number matches an existing account where the account holder has been undergone proper KYC checks, the payment amount could be credited to that account without a name-number-check requirement).
- Or based on the transmitted payee's name (as a result, the name would effectively have to be matched with the account number, which would raise a question around what should be done in case of conflict).

Both of the above interpretations give rise to questions in relation to the overall framework of Art 7 (1) to (5) as intended by FTR 2015, which is why further guidance from the ESAs is required.

It could be argued that, as long as the transaction amount is credited based on the transmitted account number to an account where the account holder has undergone proper KYC checks, the intention of FTR 2015 in this context is met:

A known ("verified") account holder would be credited. If that account holder was not the recipient actually intended by the payer, a potential money-laundering or terrorist financing attempt by the payer would in any case have failed.

In addition, this interpretation of the regulatory requirements of FTR 2015 would also be in line with civil liability rules put in place by the Payment Service Directives (PSD) 1 and 2, which allows for execution of payments based solely on account numbers.

Pursuant to PSD1, and now PSD2, the payee's PSP may credit a transaction solely based on the transmitted payee's account number to an account and will not be liable for damages in case the transmitted payee's account number is incorrect.

However, FTR 2015 imposes regulatory requirements on PSPs and as such these regulatory requirements would, as a matter of principle, prevail in this context over these civil liability rules.

4. Application of FTR 2015 on the processing of SEPA Direct Debits

In principle, direct debits are (in the same way as credit transfers) in scope of FTR 2015 requirements, since direct debits qualify as "transfers of funds" (Art 3 (9) (b)). Applied to the specifics of a private law SEPA Direct Debit (SDD) scheme, this – pursuant to Deutsche Bank's interpretation – leads to the following requirements and open questions:

a) Collections

The payee initiates the SDD via the payee's PSP that sends the collection through a "Cash Settlement Mechanism" (e.g. an automated clearing house or other mechanism) to the payer's PSP.

The collection itself is not a transfer of funds; instead it is a payment instruction (see SDD Rulebooks) as the funds are only moved on settlement day. FTR 2015, however, clearly differentiates between a "transfer of funds" and the "instruction to a transfer" and does not impose any obligations in regard to the latter. Furthermore, the information transmission requirements of Art 4 (et sqq.) are imposed on the PSP of the payer, whereas the collection is sent by the PSP of the payee. Accordingly, when applying FTR 2015 (directly), the payee's PSP has no FTR 2015-related requirements to fulfil when sending a collection.

However, taking into account the background and purpose of FTR 2015, and the legislator's clear intention to, in principle, have direct debits falling under the scope of the regulation, there may be an opportunity to consider (in theory, at least, given that clear guidance from the European Supervisory Authorities is required) an "analogue application" of FTR 2015 requirements for collections.

If this were the case, the payee's PSP, when sending a collection (the first "analogue application"), would have to comply with the information transmission requirements of Art 4 ("second analogue application"). When applying the requirements of Art 4 on the payee's PSP (instead of the payer's PSP) – and in particular when taking into account the verification requirements of Art 4 (4) and (5) – one would have to apply the information transmission requirements inversely.

In other words, the payee's PSP would have to ensure that depending on the scenario (i) the name, account number and address of the payee and (ii) the name and account number of the payer are transmitted with a collection.

Under no circumstances could it be argued that the payee's PSP has to ensure the transmission of payer's address when submitting the collection, as this line of reasoning would contravene the entire thought process taken to argue that the payee's PSP has to observe information transmission requirements when sending a collection.

b) Debit of the payer's payment account

On settlement day, the payer's PSP debits the payer's account (if the correct conditions are met, including sufficient credit etc.). However, the payer's PSP only debits the payment account of the payer and does not initiate a payment transaction to the payee. Therefore, the payer's PSP is not required to ensure that certain information accompanies a transfer to the payee as there is not, in fact, a "transfer" to the payee.

c) Settlement

Inter-bank settlement is out of scope of FTR 2015.

Further guidance from the ESAs would be welcomed as to whether, and how, FTR 2015 requirements shall be applied to SDD, in particular to the processing of collections.

Participants of the SDD scheme are recommended to process collections in accordance with the (private law) rules of the scheme. That said, participants must carefully assess – in accordance with the final guidelines – if and when information missing in a collection must be treated as a breach of FTR 2015 requirements.

Conclusion: FTR's potential impact: a call to action

To prevent unnecessary disruption to payment flows or a fragmented regulatory landscape, and, even more importantly, to ensure the safest possible regulatory framework for combating money laundering and terrorist financing, combined efforts from all stakeholders are essential.

Deutsche Bank, in its role as a market leading payments clearer and industry player, is committed to supporting the ESAs' consultancy on the guidelines crucial to achieve a common understanding and application of FTR 2015 requirements.

Despite the many practical challenges, Deutsche Bank welcomes FTR 2015's ambitions and objectives. This is a necessary progression towards enhanced anti-money laundering and counter-terrorist financing practices, which holds, above all, the safety of the society we serve as its key priority.

Deutsche Bank
Global Transaction Banking