

Wire transfers thematic examinations summary report

Issued: March 2022

Contents

Glossary of Terms	3
1 Background.....	4
2 Scope and methodology	4
3 Regulatory requirements	4
4 Key findings	5
4.1 Systems and controls	5
4.2 Corporate governance	6
4.3 Conduct of business	6
4.4 Examples of good practice observed	7
5 Questionnaire results.....	7
6 Conclusion	9

Glossary of Terms

FATF	Financial Action Task Force
Handbook	Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism
IPSP	Intermediary payment service provider means a PSP that is neither that of the payer nor that of the payee and that participates in the execution of transfers of funds;
JFSC	Jersey Financial Services Commission
Payee	Means a person that is the intended final recipient of transferred funds.
Payer	Means a person that is the holder of an account held with a PSP that allows a transfer of funds from the account or, where there is no account, a person that places an order for a transfer of funds.
PSP	Payment service provider means a person, being a person registered under the Banking Business (Jersey) Law 1991, when: <ul style="list-style-type: none"> › the person is carrying out payment services in or from within Jersey; or › being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey
Registered Person	a person registered by the JFSC under Article 9 of the BBJL to carry on deposit-taking business as defined under Article 3 of the BBJL.
Wire Transfers Regulations	EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017

1 Background

Thematic reviews are an important tool in our approach for supervising Registered Persons. By using thematic reviews to understand and assess Industry wide or sector specific risks, we aim to effectively utilise our resources by focussing on the risks that could cause the greatest harm to our guiding principles.

The domestic and cross-border payment system is vital infrastructure for our economy and financial stability. In order to prevent the misuse of the payments system, the Financial Action Task Force (**FATF**) developed recommendations, with the objective of inhibiting terrorists and other criminals from using it to transfer their funds. These recommendations also require that there are appropriate systems and controls to detect such activity, when it occurs.

Jersey's [National Risk Assessment](#) highlighted a high level of inherent risk in the value of funds transferred through Jersey Banks. This thematic examination was to help us understand whether banks have appropriate controls, have complied with regulation and are managing money laundering and terrorist financing risks effectively.

2 Scope and methodology

In November 2020, we sent out a thematic questionnaire in relation wire transfers to a wide selection of Jersey Incorporated Banks and Jersey branches of Overseas Incorporated Banks. The purpose of the questionnaire was to review and assess the extent to which banks have implemented systems and controls (including policies and procedures) to comply with the EU Legislation (Information Accompanying Transfers of Funds) (Jersey) Regulations 2017 (**Wire Transfers Regulations**), if and how firms apply exemptions and the extent and effectiveness of any monitoring.

Following the questionnaire, five banks were selected to participate in more focused examinations.

Themed examinations took place in April 2021 on a fully remote basis, with face-to-face interaction and meetings taking place using video conferencing technology.

The thematic examinations focused on assessing, inter alia, adherence to the requirements under the Wire Transfers Regulations and Section 11 of the Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism (**Handbook**).

All Registered Persons involved in the thematic have received direct feedback. Findings identified are subject to appropriate follow-up action. Follow-up action may include formal remediation plans setting out actions to be taken and timescales to complete them by. In the case of significant and material findings identified by us, this may have resulted in further escalation and in some cases further action being taken or, action may be underway.

Further information in respect of our examination program is published on [our website](#).

3 Regulatory requirements

The FATF Recommendation 16 on wire transfers with the revised interpretative note (**FATF Recommendation 16**) was implemented within the European Union by Regulation (EU) 2015/847 of 20 May 2015 on Information Accompanying Transfers of Funds (**Regulation (EU) 2015/847**).

In Jersey, Regulation (EU) 2015/847 was implemented by virtue of the wire transfers regulations with effect from 13 June 2017.

The objectives of the wire transfers regulations are:

- to prevent the abuse of fund transfers for money laundering, terrorist financing and other financial crime purposes;
- to detect such abuse should it occur;
- to support the implementation of restrictive measures; and
- to allow relevant authorities to access the information promptly.

The core requirement is that every wire transfer must be accompanied by specific (complete) information about the payer and the payee, which should be collected and retained by payment institutions, unless special exemptions and derogations apply.

A Payment Service Provider (**PSP**) should establish for each transfer of funds whether it acts as the PSP of the payer, as the PSP of the payee or as an intermediate PSP (**IPSP**). This will determine what information has to accompany a transfer of funds and the steps to take to comply with the wire transfers regulations.

PSPs are also required have effective procedures in place to detect transfers of funds that lack the required information about the payer and the payee, and to determine whether to execute, reject or suspend these transfers of funds.

4 Key findings

Weaknesses were discovered in oversight of payment operations, which might lead to senior management being unaware of issues. In total there were 18 findings with the majority of these (13) relating to gaps in systems and controls for the identification and reporting of breaches of the wire transfers regulations. There were two findings relating to weaknesses in the governance arrangements and three conduct of business issues, where controls were found to be ineffective. A summary of the issues identified follows:

4.1 Systems and controls

We consistently found that procedures lacked sufficient guidance for quantitative and qualitative measures to determine if a PSP is repeatedly failing to comply with the wire transfers regulations. Where repeated failures are detected the PSP or IPSP, must take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that PSP. These failures must be reported to us, along with details of steps taken.

All the registered persons examined, outsourced aspects of their payment processes (either to another group company or to an overseas branch of the same company, under a servicing agreement). In one case, where compliance monitoring was also outsourced, the monitoring did not include any payments made by the Jersey bank, which made up only a small proportion of transactions conducted by the service provider.

In two banks examined, it was evident that procedures had not been mapped back to the wire transfers regulations resulting in areas where procedures did not align to the wire transfers regulations.

In one case, procedures erroneously provided guidance as to derogations for making payments within the European Union, when Jersey's enactment of the wire transfers regulations had made certain amendments, one of which replaced European Union with British Islands.

In other cases, procedures lacked details as to the scope of the wire transfers regulations. This exposed the bank to the risk of failing to apply relevant processes and controls for in scope transactions.

In three cases, procedures lacked information in relation to the criminal offences for contravention of the Law.

Other findings included:

- › Insufficient details as to the definition of linked transactions and how to detect them
- › Lack of detail around information to be provided where the payer is a trustee or a company
- › Insufficient guidance as to investigation of deficient information and that this should include, amongst other matters, consideration of the customer risk assessment
- › Requirements to make a disclosure to the MLRO, where reasonable grounds for suspicion of money laundering or terrorist financing is established, not always being included in the wire transfer procedures.

4.2 Corporate governance

Two of the five banks had findings in this area, which included:

- › A lack of management information in relation to instances where payments did not contain the required beneficiary or payee information. Such management information should show whether any trends have been identified, if breaches have occurred and if any necessary notifications have been made to us. Where management information was provided, this predominantly related to payment volumes and timeliness.
- › Business Risk Assessments lacked sufficient detail as to the risks associated with relevant payment channels, including money laundering or terrorist financing typologies and did not adequately explain the bank's risk based approach in the design of its controls, and in its conduct of on-going monitoring.

4.3 Conduct of business

All of the banks examined had in place controls to detect and remediate instances where required information was missing from payments. Whilst the controls in place to detect missing information were operating effectively, there were failings in the controls in place to ensure appropriate remediation.

In one case, a bank had identified that required information was missing from an incoming payment, however, the bank failed to make enquiries with the US remitting bank and repair the defects.

In another, we noted that a bank had omitted required information and then failed to respond to payment information requests in a timely manner.

Despite detecting payments without the required information, banks were not consistently recording these as a breach of the wire transfers regulations.

4.4 Examples of good practice observed

- › Core banking systems automatically populated required payment information into outward payment messages
- › Automatic scanning of incoming payments to detect any missing information
- › Periodic sampling of payments was undertaken to detect issues with controls
- › Use of a central team responsible for investigating incomplete information and maintaining a central log of all investigations and outcomes.

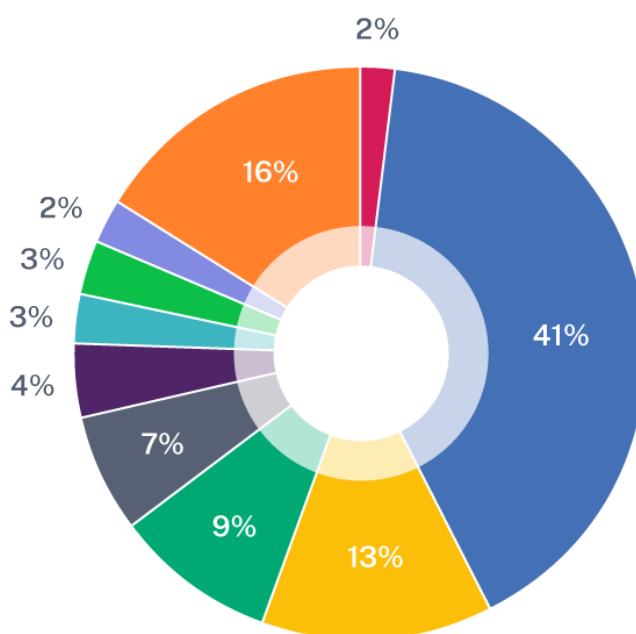
5 Questionnaire results

We sent thematic questionnaires to 17 banks with responses received in December 2020. The responses were reviewed in conjunction with Supervisory Risk Data we hold, in order to identify banks for inclusion in the on-site examinations. This review included consideration of responses in comparison to the requirements of the wire transfers regulations, as well as FATF Recommendation 16 and its guidance.

Where the review identified matters in respect of banks that were not chosen for on-site examinations, follow-up queries were raised to those banks in April 2021.

At the time of the review, our Supervisory Risk Data indicated that during 2019, Jersey's banks received over 2.2million inbound wire transfers totalling £385bn, of which 78% by value were from Europe and the UK and a further 14% from North America. Jersey's banks made over 2.4m outbound wire transfers totalling £365bn, with 69% by value made to Europe and UK and a further 22% to North America.

Origin of incoming payments



Transfers to or from countries appearing on [Appendix D2](#) of the Handbook account for just 2% of wire transfers by value in 2019.

Analysis of questionnaire responses identifies that, whilst all banks surveyed act as PSPs only two banks (12%) confirmed they act as an IPSP. None of the banks surveyed provided non-account holders with the ability to make payments or transfer funds.

All respondents indicated they had implemented policies, procedures and controls to ensure compliance with wire transfers regulations; 13 banks (76%) indicated that these processes and controls had been tested within the last three years. All respondents indicated that their payment procedures include controls to prevent wire transfers being made without the mandatory information being transmitted.

Only six banks (35%) indicated that they took advantage of one or more of the derogations available in the wire transfers regulations in respect of transfers within the British Islands (UK, Jersey, IOM, Guernsey) or where transfers do not exceed EUR1,000.

Only seven banks (41%) indicated that they process batch file payments and all of these confirmed that batch files were required to include the information required by the wire transfers regulations.

All banks indicated that they had implemented monitoring processes to detect inbound transfers that are missing mandatory wire transfer information. 15 banks (88%) indicated that this monitoring included use of automated systems. Monitoring was predominantly comprised of automated real-time or manual post-event monitoring, with some banks also utilising automated post-event monitoring. Nine banks (53%) used a combination of two or more methods of monitoring to detect inbound transfers with missing information. 12 banks (71%) outsourced this monitoring activity elsewhere within their groups, typically to centres of excellence.

No banks indicated that the monitoring of wire transfers had directly resulted in internal suspicious activity reports being made to the Jersey based Money Laundering Reporting Officer (MLRO). This raises a concern that either the monitoring is not effective at identifying wire transfers that give rise to suspicion or group centralised employees are raising their suspicions to MLRO's in the country in which they are located, without them being passed on to the Jersey MLRO. There is a risk that these monitoring activities focus only on identifying missing information, remediating that missing information and/or rejecting transfers, so that the missing information is not considered as a factor when assessing whether the transfer of funds, or any related transaction, is suspicious (a requirement of Article 9 of the wire transfers regulations).

11 banks (65%) confirmed that they had policies and procedures in place to deal with PSPs that repeatedly failed to provide the required information on the payer or the payee. Of the six banks (35%) that did not have policies and procedures for this, one (a branch of an overseas Incorporate Bank) noted that this activity is performed at a group level only and four explained that there had never been a need for such procedures because, in their experience, instances of missing or incomplete information were very infrequent. This view was not supported by the outcome of our examinations, which discovered instances of payments lacking complete information and that in some cases group procedures had not been mapped to Jersey's regulations.

13 banks (76%) outsource activities relating to repeatedly failing PSPs either to group centralised functions or other entities/branches within their groups.

None of the respondents indicated that they had taken action in the last 24 months to reject future payments or terminate the business in respect of a repeatedly failing PSP.

No banks indicated that there had been breaches of the wire transfers regulations in the last 12 months. At the same time, two banks (12%) explained that instances of outbound transfers containing missing or truncated information had been identified. This was a result of failures in banks' processes to record breaches where outbound transfers were found to have missing or incomplete information.

6 Conclusion

It is evident that banks in Jersey have developed advanced controls, including automated systems, to comply with the wire transfer regulations to reduce the risk of criminals using payment systems.

Nevertheless, our thematic review has uncovered instances where controls have not always been operating effectively or where assurance work undertaken by compliance or internal audit, has not included an assessment against the regulatory requirements in Jersey.

A contributing factor for issues arising appears to be the outsourcing of activities (either to a group company or to an overseas part of the same company).

In light of these findings, we expect Registered Persons to:

- › review relevant outsourcing arrangements, whether to another group company under an outsourcing agreement or an overseas branch of the same company, under a servicing agreement. In respect of the former, this should include ensuring that our outsourcing policy guidance note is complied with
- › ensure that procedures comply with the wire transfers regulations and that any breaches are being recorded and managed appropriately, which must include reporting of repeated breaches to us.