



# **TYOLOGY**

## Money Laundering Scheme - Russian Laundromat

---

May 2022

# Typology Report

Money Laundering Scheme – Russian Laundromat

Financial Intelligence Agency (FIA) – Bermuda

CONFIDENTIAL

May 2022

## Statistical Disclaimer:

The report's statistics are based on SARs and STRs submitted to the FIA between January 1, 2019 and March 31<sup>st</sup>, 2022. These reports reflect suspicions from reporting entities and do not confirm the existence of criminal activity. The data is intended for analysis and may change as new information or investigations arise. While reasonable steps are taken to ensure accuracy, the FIA relies in part on information provided by reporting entities and other third parties and cannot independently verify all underlying data.

**Contents**

Introduction ..... 3

*Indicators and Red Flags* ..... 3

*Typology Objectives* ..... 3

The Russian Laundromat ..... 4

    What is the Russian Laundromat? ..... 4

    When was the Russian Laundromat first detected according to OCCRP? ..... 4

    What is the purpose of the Russian Laundromat according to OCCRP? ..... 4

    Who was behind this system according to OCCRP? ..... 4

    What did the transactional activity look like according to OCCRP? ..... 4

    Statistical Overview ..... 5

Reporting Indicators ..... 5

SAR/STR reviews ..... 5

    STR Review 1- Suspected Money Laundering - Russian Laundromat ..... 6

        Reporting Sector: Long-Term Insurers ..... 6

    SAR Review 2- Suspected Money Laundering - Russian Laundromat ..... 6

        Reporting Sector: Investment Service Providers (ISPs) ..... 6

    STR Review 3- Suspected Money Laundering - Russian Laundromat ..... 6

        Reporting Sector: Long-Term Insurers ..... 6

    SAR Review 4 - Suspected Money Laundering - Russian Laundromat ..... 7

        Reporting Sector: Long-Term Insurers ..... 7

Red flags ..... 7

Actions taken by Reporting Entities ..... 9

## Introduction

In January 2020, Bermuda received a glowing report from the Caribbean Action Task Force (CFATF) and the Financial Action Task Force (FATF) due to the robustness and effectiveness of its AML/CFT regime and legal framework in accordance with the international standards promoted by the FATF's 40 Recommendations and associated Methodology.

As a result, Bermuda endeavours to continue promoting AML/CFT awareness and training, as well as conducting ongoing reviews and revisions of Bermuda's AML/CFT framework in order to more effectively detect and deter opportunities that criminals seek to launder the proceeds of crime.

Likewise, it is paramount that local reporting entities, reporting persons and stakeholders remain aware of emerging and persistent patterns and trends to best address incidents of money laundering and terrorist financing within the Bermuda economy.

To meet these objectives, the FIA has produced a typology to discuss indicators highlighted in Suspicious Activity Reports (SAR), Suspicious Transaction Reports, Incoming Requests for Information (IRIs) and other intelligence reports filed by local reporting entities, local competent authorities and Egmont Financial Intelligence Units (FIUs). This typology covers reports filed between January 1st, 2019, and March 31st, 2022.

This typology focuses on a suspected money laundering scheme known as the Russian Laundromat. Case studies, suspicious indicators, statistics and the actions taken by the filers in response to the red flags presented. These elements have been included in this report to provide clarity, insight and suggestions when dealing with cases of this nature.

## Indicators and Red Flags

Report indicators can provide insight into various patterns and trends that are taking place locally and internationally when chosen within SAR/STR/UTR filings. When reporting entities select relevant indicators, this enables FIA analysts to conduct analysis more effectively, widening the scope during the information/intelligence gathering, collation and synthesis processes of the intelligence cycle. Ultimately, this information enables the FIA to readily produce more case studies and typologies to share locally and internationally.

## Typology Objectives

The following objectives are intended to be achieved through the dissemination of FIA Typologies:

- To identify potential and actual illegal activity associated with money laundering, terrorist financing and other predicate offences.
- To educate reporting entities, reporting persons, local and overseas competent authorities, financial intelligence units (FIUs) and the public about the various methods and techniques that criminals may use to launder the proceeds of crime.
- To identify areas that need added attention and that assist in the detection, prevention, investigation and prosecution of higher-risk opportunities that require regular or ongoing monitoring; and
- To establish emerging and persistent threats through analysis of patterns and trends.

## The Russian Laundromat

### What is the Russian Laundromat?

According to The Organized Crime and Corruption Reporting Project (OCCRP), this system is "...an immense financial fraud scheme that enabled vast sums to be pumped out of Russia. The money was laundered and moved into Europe and beyond through bribery and a clever exploitation of the Moldovan legal system."<sup>1</sup>

### When was the Russian Laundromat first detected according to OCCRP?

OCCRP in its investigative project described how during 2010 and early 2014, organized criminals and corrupt politicians in Russia moved USD 20 billion in dirty funds through a complex cleanse-and-spin cycle made up of dozens of offshore companies, banks, fake loans, and proxy agents referred to as the laundromat. Judges from Moldova would then solidify the process as cleansed and the newly cleaned funds were then spread across Europe.<sup>2</sup>

### What is the purpose of the Russian Laundromat according to OCCRP?

OCCRP further explored how the continued problem with the dirty money was explaining where it comes from. According to its journalists crime is mostly a cash economy, and mobsters or dirty government officials often find themselves with massive piles of cash they prefer not to explain—especially to tax officials.

The Laundromat scheme was constructed to create a false impression of legitimate business activity offering an explanation for the origin of the funds. Court approvals were used to validate the transactions and make them appear lawful.

In reality, OCCRP surmised that the supposed businesses involved were merely shell entities masking the identities of the true owners.

### Who was behind this system according to OCCRP?

"The banks and companies involved are run by managers and board members that include well known businessmen, a cousin of Russian President Vladimir Putin, and persons said to be close to the KGB."<sup>3</sup>

### What did the transactional activity look like according to OCCRP?

According to journalists from the OCCRP, a typical transaction within the scheme involved two companies registered in the United Kingdom, whose real ownership was concealed through offshore structures. These companies would enter into a fraudulent loan agreement involving extremely large sums, despite no funds actually being exchanged. OCCRP reporting suggests that both companies were usually controlled by the same hidden owner, whose identity was obscured by proxy individuals.

OCCRP journalists, using Belize as an example, explored how such tax havens could be used for loan amounts ranging between USD 100 million and USD 800 million. Each agreement included a guarantee from Russian-registered companies, often managed by a Moldovan national—an arrangement that enabled the organisers to bring the fabricated dispute before Moldovan courts and thereby legitimise the movement of illicit funds.

As described by OCCRP, the "borrowing" company would then default, transferring

<sup>1</sup> The Russian Laundromat Exposed. Organized Crime and Corruption Reporting Project (OCCRP). August 22, 2014. <https://www.occrp.org/en/project/the-russian-laundromat-exposed>

<sup>2</sup> The Russian Laundromat - Investigation. August 22, 2014. <https://www.occrp.org/en/project/the-russian-laundromat/the-russian-laundromat>

<sup>3</sup> The Russian Laundromat - Investigation. August 22, 2014. <https://www.occrp.org/en/project/the-russian-laundromat/the-russian-laundromat>

responsibility for repayment to the Russian guarantor. This would trigger court action in Moldova, where a judge would validate the debt and order repayment. The Russian company would subsequently transfer illicit funds to an account held by the “lending” company, with transfers consistently routed through Moldindconbank—an institution linked to influential Moldovan business figures.

Finally, OCCRP journalists reported that the funds were forwarded to an account at Trasta Komercbanka, a bank in Latvia. Once the money entered Latvia’s banking system, supported by a court order, it essentially became integrated into the EU financial system and appeared as legitimate funds.

To read more about the Russian Laundromat scheme, please refer to these websites:

1. <https://www.occrp.org/en/laundromat/>
2. <https://www.occrp.org/en/laundromat/russian-laundromat/>

### Statistical Overview

Upon a review of the FIA database (goAML) for the period of January 1st, 2019, and March 31st, 2022, it was identified that four (4) SARs were filed involving a suspected money laundering scheme known as the Russian Laundromat. A breakdown of these filings per year and per Reporting Sector is shown in Tables 1 and 2.

Table 1: Number of Filings Involving the Money Laundering Scheme - Russian Laundromat

Year	No. of Local SARs Filed	No. of Local STRs Filed	No. of International IRIs Filed	TOTAL
2019	2	0	0	2
2020	0	0	0	0
2021	1	0	0	1
2022 (Jan - Mar)	1	0	0	1
<b>TOTAL</b>	<b>4</b>	<b>0</b>	<b>0</b>	<b>4</b>

Table 2: - Russian Laundromat Filings by Reporting Sector

Reporting Sector	# of Filings
Investment Service Providers (Non-Regulated)	1
Banks	1
Long-Term Insurers	2

\*One of the long-term insurers also files dually with another jurisdiction.

### Reporting Indicators

Indicators of suspicious activity selected by reporting entities when filing SARs/STRs, by year, that involved the suspected money laundering scheme, Russian Laundromat, are shown below.

2019	2021	2022
Adverse Media	Beneficial Ownership	Adverse Media
Beneficial Ownership	Bribery	Corruption
Company	Closed Account / Policy - suspected criminal activity	Criminal History
Criminal History	Company	Declined/Refused business - suspected criminal activity
Declined/Refused business - suspected criminal activity	High Risk Country	High Risk Country
Drug Trafficking/Activity	Inadequate/Evasive Explanation	Investment Related
For Information Only	Inconsistent Account Activity	Money Laundering
Fraud	Money Laundering	PEP Foreign
High Risk Country	Previous filings on subject/entity	Russian Laundromat
Inconsistent Account Activity	Use of Insurance Products	10. Tax evasion
Legal Arrangements	Wires	
Misrepresentation		
Money Laundering		
Ongoing monitoring		
PEP Foreign		
Police Production Order / FIA Notice to Provide Information		
Refusal to comply with KYC requirements		
Sanctions List		
Shell Companies		
Use of Insurance Products		
Wires		

### SAR/STR reviews

In order to illustrate the content and context of reports filed with the FIA suspected to have involved the Russian Laundromat, four (4) SAR/STR reports filed by the three reporting sectors were reviewed. Through these reviews, suspicious activity and red flags were identified to help with the prevention, detection and investigation of this suspected money laundering within the Bermuda economy.

### STR Review 1- Suspected Money Laundering - Russian Laundromat

#### Reporting Sector: Long-Term Insurers

Reason for Suspicion: In 2017 and again in 2018, the reporting entity received a preliminary life insurance application for a subject, noted to have been a PEP, as a proposed insured. The application in 2017 was subsequently declined, and the subject did not become a policyholder. As a result, client due diligence was not required nor obtained and therefore minimal information was received on the subject.

The preliminary application in 2018 was also declined on the basis of an elevated reputational risk. Upon a review of the application, it was identified that the subject was the co-owner/founder/shareholder of a multitude of companies, many which were linked to adverse media related to the Russian Laundromat scheme and sanctions.

### SAR Review 2- Suspected Money Laundering - Russian Laundromat

#### Reporting Sector: Investment Service Providers (ISPs)

Reason for Suspicion: Adverse media was found on a Moldovan national, who applied for a trading account with the ISP. Following the submission of the new account application, negative media was identified during client screening. It is believed that the applicant was likely a potential match with a subject of negative media due to the date of birth referenced on the application. The date of birth matched that of the subject of the adverse media provided in the screening software.

Online searches were conducted during client screening and characteristics of these findings were as follows:

- Previous involvement in a money laundering scheme e.g. Russian Laundromat
- Suspicion of tax evasion

- Suspicion of colluding with rogue government officials

The subject's trading account application was rejected by the ISP, and no deposit or deposit attempts were made by the subject to fund an account. Additionally, the ISP blacklisted and banned the subject from further dealings.

Given the seriousness of the concerns identified in the adverse media, the ISP filed a SAR not only to notify the FIA of the subject's attempt to open a trading account but also to furnish information related to the subject's whereabouts and contact information.

### STR Review 3- Suspected Money Laundering - Russian Laundromat

#### Reporting Sector: Long-Term Insurers

Reason for Suspicion: A transfer of ownership request was received from an existing policyholder, TNT Ltd., to transfer the policy ownership to another company, JBL Ltd. Several red flags were identified within the request. TNT Ltd. Was noted to be a company registered in Central America with contacts in Europe and no contacts were provided for Asia, the jurisdiction where the reporting entity was based. The reason provided for TNT Ltd. to operate an account in Asia appeared dubious as well.

According to bank account records, TNT Ltd. conducted transactions with counterparts located in high-risk countries; some of which were subjects of previous FIA disclosures. Additionally, they appeared to have a connection with each other. The beneficiary owner of TNT Ltd. was noted as a Russian national, whose personal details were a match with the actors of an alleged money laundering scheme (i.e. Russian Laundromat"). This scheme revolved around loans between UK front companies guaranteed by a Russian individual or company. When such loans were defaulted on, repayment was sorted through Moldavian courts. The Russian guarantor would then be

ordered to repay the funds, thereby legitimizing the money with a court order for subsequent routing to the UK, and to the reporting entity.

JBL Ltd. provided a deed of gift as a supporting document for the policy transfer. However, no connection (e.g. nature of business, beneficial owner, place of business) between the existing and proposed policy holder was found. JBL Ltd. was previously exited by the reporting entity due to suspicious activity identified from another company owned by the same UBO.

#### SAR Review 4 - Suspected Money Laundering - Russian Laundromat

##### Reporting Sector: Long-Term Insurers

Reason for Suspicion: This SAR was submitted in relation to several suspicious transactions conducted between accounts at a local bank between 2012 and 2018 that were introduced by the same financial service provider.

One of the companies Psalm Company, involved a client domiciled in Bermuda with a UK address and the other, ABC Company, was a Bermuda company. During a review of Psalm Company's accounts in 2018, it was discovered that several KYC documents were missing. The client was then contacted to submit those missing documents. Before providing them, the client instructed that several of the accounts be closed. A review conducted by the bank's compliance team identified that some of the accounts had made suspicious transfers. It was then identified that funds were wired to a shell company in Latvia. Further investigations revealed that the shell company had corporate directors that were also shell companies. One of the connected persons, a Russian national with significant control, held no information available on file. Based on this suspicious activity, the bank likened it to global laundromat typology through the use of shell companies and Latvian bank accounts to transfer criminal proceeds.

Suspicious transfers were also made from Psalm Company accounts to a shell company registered in the Seychelles with bank accounts held in Cyprus. The purpose of these payments varied, although most indicated reasons such as salaries, expenses, or fees including for legal services.

On examination of the documents on file relating to Psalm Company, it was discovered that documents provided by Psalm Company were linked to a namesake trading subsidiary, which held a registered address in Cyprus. Some of the Directors of the trading subsidiary were linked to significant negative news connected to Russian money laundering allegations.

Payments were also sent from the accounts of ABC Company to South America. Negative news with links to a drug trafficking ring was found in relation to one of the wire recipients. No further updated information was found. Another payment from the accounts of ABC Company made no economic sense as the payment was made to a fishing company using a reference for a textile entity. Other payments were received from South American shell companies with bank accounts in Europe. Further investigations revealed that the fishing company was a potential match for a fishing company that operated in Europe and was acquired by the Psalm Company group in 2011.

Further connections were made between bank clients who sent and received funds linked to Psalm Company and were also managed by the introducing financial services provider. It must also be noted that there was previous interest from the Bermuda Police Service into the introducing financial service provider.

#### Red flags

Red flags noted in some of the filings involving the suspected Russian Laundromat were as follows:

- Adverse media identified on World Check was found on the subject, business associates, and related companies.
- Adverse media identified via open-source articles was found on the subject, business associates, and related companies.
- The applicant was a potential match with the subject of negative media due to the date of birth referenced on the application, and which matched the date of birth within the adverse media provided by the screening software.
- The company was registered in Central America with contacts in Europe and no local contacts in Asia where the reporting entity was based. The reason for the company to operate an account in Asia is dubious.
- The company transacted with counterparts located in high-risk countries.
- Some of the companies that the company transacted with were previously disclosed to the FIA and apparent connections between the companies were evident.
- The beneficiary owner of the company was a Russian who was a match with the actors of a typology of a money laundering scheme i.e., Russian Laundromat.
- The proposed policyholder, a company, provided a deed of gift as a supporting document of the policy transfer.
- No connection between the existing policyholder, a company, and the proposed policyholder, another company, could be identified.
- The proposed policyholder, the company, had been previously exited by the reporting entity due to suspicious activity identified which was linked to a sister company owned by the same UBO.
- The insured person of the policy would have remained unchanged. However this person held no relationship with the proposed policy holder.
- The subject's preliminary life insurance application was previously declined on the basis of elevated reputation risk.
- The subject did not provide a home address at the preliminary application stage possibly to hide the subject's current location.
- The subject purportedly benefitted from the alleged Russian laundromat scheme.
- The SAR was submitted in relation to several suspicious transactions conducted between accounts at the bank introduced by the same financial service provider.
- During a review of the company's accounts, it was discovered that several KYC documents were missing. Once the client was contacted to provide the required documents, the client instructed that several accounts be closed.
- Wires were sent to shell companies that were owned by shell companies.
- Some of the shell companies were registered in high-risk countries.
- The Directors of the trading subsidiary of the Bermuda registered client that held a local bank account was linked to significant negative news connected to Russian money laundering allegations.
- The Bermuda Police Service had previously expressed interest in other companies introduced to the bank by the financial service provider.
- Open-source checks linked the wire payment of the Bermuda company to a person in South America linked to negative news suggesting possible involvement in drug trafficking.
- The type of company in receipt of the wire payment, a fishing company, did not match a reference for textiles observed amongst payments.
- The transactions were unusual as they were sent from a South American shell company with bank accounts in Europe.
- Further connections were made between bank clients who sent and received funds linked to the company and are also

managed by the introducing financial services provider.

- Further investigation revealed that the fishing company that sent funds to the company with a reference for textile was a potential match for a fishing company that operated in Europe and was acquired by the Psalm Company group in 2011.

#### **Actions taken by Reporting Entities**

- The subject's trading account application was rejected.
- The subject was blacklisted and banned from further dealings with the reporting entity

- A SAR was filed to furnish information related to the subject's whereabouts and contact information in addition to the subject's trading application.
  - The subject did not provide a home address.
  - The existing policyholder, a company, was exited due to suspicious sources of funds which originated from a suspicious proposed policyholder, also a company.
  - The subject's preliminary life insurance application was declined due to adverse media, which presented an elevated reputation risk.
  - The filing was for acknowledgment only.

END