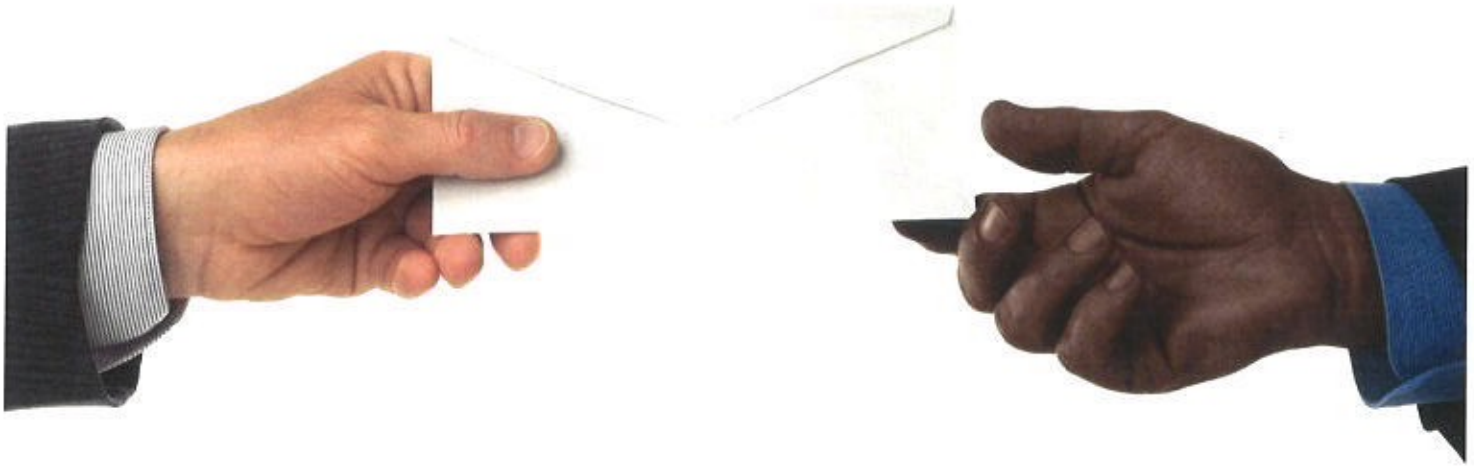
FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

Intelligence Assessment

Moscow Mirror Network Demonstrates Anti-Money Laundering Vulnerability in Global Securities Market



FinCEN Intelligence Assessment

Law Enforcement Sensitive/Contains BSA Information

INTELLIGENCE DIVISION

Moscow Mirror Network Demonstrates Anti-Money Laundering Vulnerability in Global Securities Market

Executive Summary: *Mirror trading—a foreign exchange strategy that uses offsetting securities trades across different jurisdictions—highlights a vulnerability in the global securities market for money laundering. A network of Russian-based individuals and entities, herein the "Moscow Mirror Network," have used this method as an informal value transfer system (IVTS) to move billions of dollars per year from Russia through European securities markets to other jurisdictions beginning as early as 2011. Since this network used mirror trading to conduct illicit financial activity, law enforcement and regulators are encouraged to review collections of securities trades for red flags that may detect suspicious uses of mirror trading.*

Mirror Trading Allows Concealed Transfers of Funds across Borders

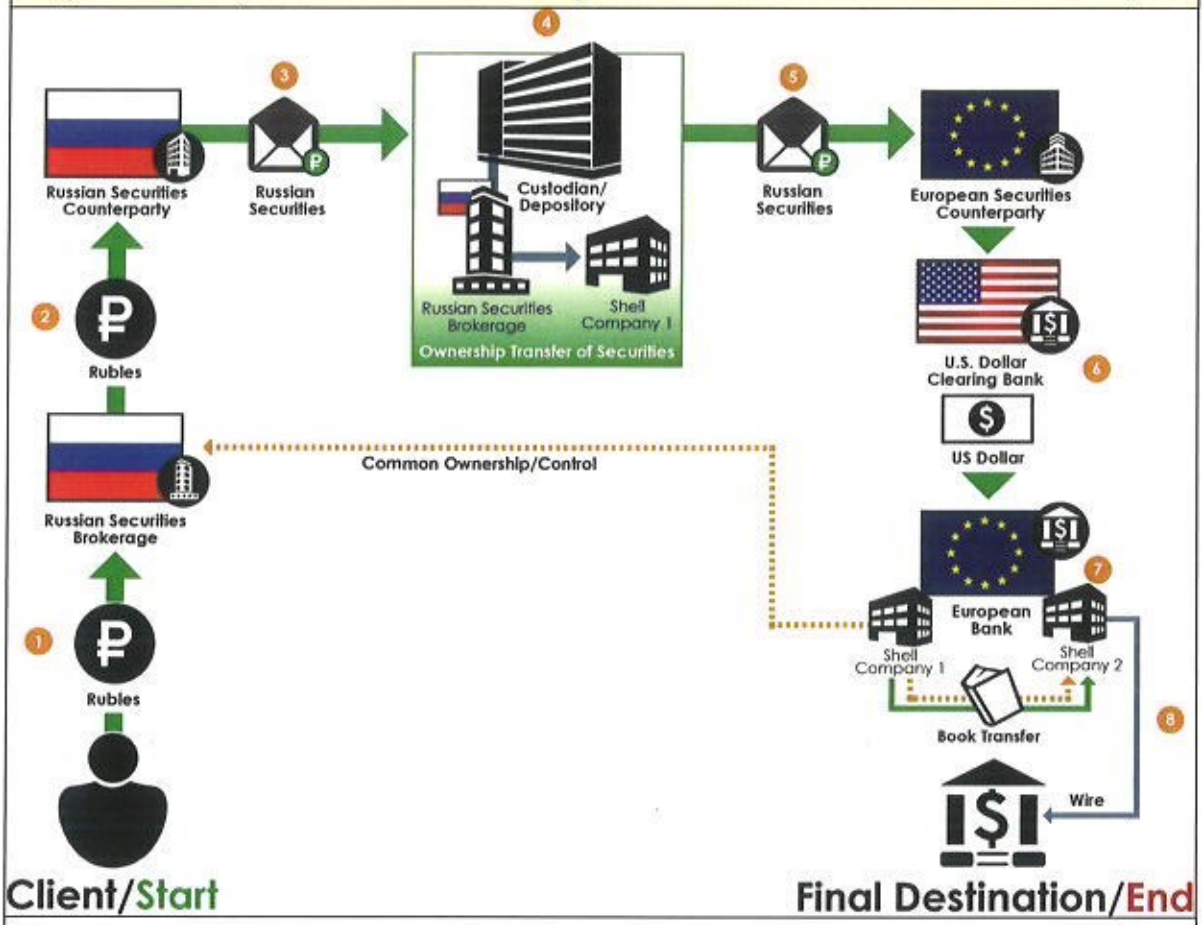
Mirror trading is an informal value transfer mechanism through which an individual or business purchases securities in one jurisdiction and sells them in another for no economic gain, thereby concealing the funds' original source and final destination. Although not inherently illegal, mirror trading is being used to move funds out of one country by converting domestically-held currency into euros, British pounds, or U.S. dollars through a sophisticated layering process involving two simultaneous, or near-simultaneous, securities trades.

Mirror trading can be conducted through a variety of approaches, but one common process is as follows: First, an individual, or "client," requests that a mirror trading network move money out of one country into another jurisdiction. The network uses the client's funds in its original currency to make over-the-counter purchases of liquid, blue-chip securities on the client's behalf through a securities brokerage. The ownership of the securities is transferred to a shell company, which is often registered in a jurisdiction at higher risk for money laundering.

Soon after the initial securities purchase, the offshore shell company sells the securities over-the-counter to a broker-dealer located in another jurisdiction. The sale is conducted in the desired currency, such as euros, British pounds, or U.S. dollars. The broker-dealer then sends the proceeds to the shell company's bank account, which is likely located in a jurisdiction that specializes in non-resident or offshore banking.

Once converted into the desired currency, the funds are often transferred to additional shell company accounts using book transfers within a bank or via wire transfers to another bank. The funds are ultimately wired to a bank account as directed by the original client. As a result of this process, the identity of the transaction's true originator is hidden from Western financial institutions, which are likely only aware of the sale of securities by an offshore firm to a European broker.

Figure 1: Example of How Mirror Trading Can Transfer Funds from Russia to Europe



Step 1: A client requests that a mirror trading network transfers rubles located in Russia abroad.
Step 2: A network-controlled securities brokerage purchases securities on behalf of the client from a securities counterparty in Russia.
Step 3: The securities counterparty in Russia transfers the securities to the network-controlled securities brokerage.
Step 4: The network-controlled securities brokerage transfers ownership of securities to an offshore shell company controlled by the network.
Step 5: The shell company sells the securities to a securities counterparty in Europe.
Step 6: The securities counterparty sells the securities on behalf of the shell company and puts the sale proceeds in the shell company's bank account.
Step 7: The shell company moves the sales proceeds through a book transfer or wire transfer to another network-controlled shell company.
Step 8: The funds are transferred to a bank account as directed by the client.

FinCEN's knowledge of the mirror trading method is primarily derived from information about the Moscow Mirror Network. Figure 1 and the corresponding steps above demonstrate how Deutsche Bank—acting as one of the securities counterparties in Russia and the United Kingdom—observed the Network transfer funds from Russia to Europe.

Moscow Mirror Network Transfers Billions of Dollars Using Russian and European Securities Markets

Four key individuals have used mirror trading to transfer billions of dollars per year, and at least $1 billion per month in some instances, from Russia to other jurisdictions and, at times, on behalf of illicit actors. In an apparently ongoing process, these individuals, who have engaged in suspicious behavior, ensure that the funds transfers are processed opaquely for a fee of up to five percent.

FinCEN assesses that these individuals and entities constitute a network, involving at least 54 shell entities and nine financial institutions (see Attachment A). This "Moscow Mirror Network" (or "the Network") purchased Russian blue-chip securities—[redacted] stocks and bonds—and sold them on the European market to well-known firms, such as Deutsche Bank, [redacted], and [redacted]. Key European counterparties of the Network include Schildershoven Finance and Tristane Capital B.V. of The Netherlands, Baltic Credit Trading Group of Latvia, and [redacted].

Figure 2: Key Individuals in the Moscow Mirror Network

Andrey Yurievich Babenko is a Russian stockbroker.

Babenko had shared or complete ownership of two Network entities. He was also a director at [redacted], the London branch of a Russian brokerage firm to which the Network later sold securities.

Oleg Aleksandrovich Belousov is a Russian bank owner and executive.

Belousov had shared or complete ownership of 24 Network entities, many of which he shared with Kulikov.

Andrey Vladimirovich Gorbatov is a Russian stock and equities trader.

Gorbatov had shared or complete ownership of four Network entities, including RMG Securities, a Russian securities brokerage through which the Network purchased securities.

Alexey Anatolevich Kulikov is a Russian businessman and bank executive.

Kulikov had shared or complete ownership of 26 Network entities, many of which he shared with Belousov. He was detained on 3 March 2016 for two months at the request of the Russian Interior Ministry on financial crime charges.[1]

The entities involved in the securities trades share common characteristics—such as ownership, place of registration, and banking location—suggesting that they may have acted in concert with each other to formulate the process of moving the

funds out of Russia. Three examples of shared characteristics between Network entities are as follows:

- **Common Banks:** Forty-six of the 54 shell entities held accounts at one or more of the following banks: Trasta Komercbanka (Latvia), Danske Bank (Estonia), and Cyprus Development Bank (Cyprus)—the latter formerly majority-owned by Kulikov, Belousov, and Gorbatov. Four of the entities also held accounts at Promsberbank, which was partially-owned by Kulikov and Belousov.[2]
- **Common Ownership:** The four key individuals have shared or complete ownership of 32 Network entities. Furthermore, [redacted] Igor Marakin, and attorney [redacted] repeatedly appeared on company records; for example, as the Network entities' ultimate beneficial owners, attorneys, and shareholders.
- **Common Addresses:** The reported physical addresses and places of registration were also shared between the Network entities. For example, out of the 34 entities with reported addresses, nine of them are reportedly located at 22 Begovaya Street in Moscow.[3]

The Network and Its Clients Involved in Suspicious Activity

Network individuals and entities have histories of anti-money laundering violations and direct involvement in mirror trading scandals. For example:

- Deutsche Bank fired three employees in April 2015 related to a $10 billion mirror trading scheme.[4] Deutsche Bank identified that 13 Network entities were part of this scheme.[a 5] Kulikov was detained for two months at the request of the Russian Interior Ministry, and the Russian Central Bank revoked the license of Network brokerage RMG Securities for related allegations.[6]
- In July 2015, the Central Bank of Russia revoked the license of Promsberbank, which was partially-owned by Kulikov and Belousov, after determining the bank had inappropriately transferred 1.3 billion rubles, or approximately $21,268,000, to a foreign insurance company that was ultimately determined to be a shell company.[b 7]

---

[a] Deutsche Bank identified the following entities as part of The Network: [redacted], Bonnicrest Management Limited, [redacted], Chadborg Trade LLP, Cherryfield Managment Ltd., Ergoinvest LLP, [redacted], Financial Bridge Investment Company, [redacted] OSJC Ray Man Gor Securities, and [redacted].

[b] The conversion from rubles to U.S. dollars is based on the July 31, 2015 close of .01636 RUB/USD from xe.com.

- In 2011, Russian regulators suspended [redacted] and Financial Bridge Investment Company—two financial brokerages involved in the Network's mirror trading activity—related to a value added tax fraud scheme totaling 3.2 billion rubles, or approximately $99,776,000, via over-the-counter securities transactions.[c 8 9]

Some of the Network's suspected clients have also been involved in suspicious or illicit activity. Forty-one of the top fifty entities that received funds from the Network were subjects of sensitive financial reporting obtained by FinCEN, and some recipients have been designated by OFAC or convicted of criminal activity, indicating that at least a portion of the Network's mirror trading likely was conducted for illicit purposes.[d] For example:

- OFAC-designated Mazaka General Trading LLC (Mazaka) received a total of $49,787,832 from five Network entities between March 2013 and April 2014. In October 2016, OFAC sanctioned Mazaka for having materially assisted, sponsored, or supported the Khanani Money Laundering Organization, which launders illicit funds for terrorists, drug traffickers, and criminal organizations.[10]

- LA Payroll, which was implicated in an alleged tax fraud scheme in the United States in 2014 with an estimated total loss of $4 million, sent a wire for $480,000 to Network entity Redwind Experts LLP in August 2013.[11]

- Eurasian organized crime-linked Gurgen House FZCO received a total of $810,000 from two Network entities—Bolzana LLP and Aronica Alliance LTD—in September 2011 and February 2012.[12] OFAC designated Gurgen House FZCO in October 2013 for ties to the Brothers Circle Organization, a Eurasian criminal group involved in drug trafficking.[13]

Additional Factors Concealed Illicit Behavior

As part of the Network's mirror trading activity, banking records in Russia reflected the domestic purchase of securities, while banking records in Europe recorded an intra-European purchase of securities. This cross-jurisdictional separation of recordkeeping largely hid the true nature of transactions from U.S. dollar-clearing institutions, and obscured individual transactions from other financial institutions involved in the process.

The Network further eroded transparency by establishing entities with shell-like characteristics and layers of ownership, and by conducting book transfers to hide

---

[c] The conversion from rubles to U.S. dollars is based on the Dec 29, 2011 close of .03118 RUB/USD from xe.com.

[d] FinCEN ranked the recipients of funds from the Network entities and brokerages and then removed banks and cities listed in the results to determine the top fifty entities that received funds from the Network.

who was involved in the Network and for whom the funds were being transferred. For example:

- **Use of Book Transfers:** The Network used inter-account fund transfers within the same financial institution, or book transfers, between Network entities to further hide the money trail and the identities of its clients. These transfers are recorded for accounting purposes, and therefore are not monitored through the financial system.

- **Use of Shell Entities:** Fifty-six Network entities have shell-like characteristics, such as being engaged in non-proximate banking and being registered in higher-risk jurisdictions for shell company formation, such as Cyprus and the United Kingdom. For example, nine entities are registered to 175 Darkes Lane in London, one of the most common foreign addresses in FinCEN's sensitive financial reporting.[e] [f]

- **Layers of Ownership:** The Network further hid transactions through layers of shell companies and nominee shareholders. For example, a key Network-controlled securities dealer, [redacted], was owned by Babenko and Gorbatov through nesting ownership of two other Network entities, Cherryfield Management Limited and Ventarre Limited.[14] [15]

Indicators of Mirror Trading

Mirror trades are not inherently illegal and, as individual trades, do not necessarily appear suspicious. For example, purchasing securities in one country and selling them in another is a legitimate way for clients to benefit from the difference between local and foreign prices of a stock. Mirror trading can also help a securities brokerage comply with country capital controls.

Mirror trades, however, can be used to facilitate illicit financial activity—to include money laundering, sanctions violations, and tax avoidance—because of the lack of transparency. Although the Moscow Mirror Network is operating in Russian and European securities markets, other jurisdictions are also vulnerable to illicitly motivated mirror trades. Another network, for example, appears to have moved money out of China and into the United States using offsetting securities trades.[16] In this example, an employee at U.S.-based [redacted] indicated his concerns about the securities trades were "wash and prearranged

---

[e] Non-proximate banking refers to when an entity is registered in a location that is different from the location of its bank account.

[f] In an Executive Alert titled "Panama Prominent in Top Addresses for Shell Company Formation" (FIR # [redacted]), FinCEN identified the ten most-commonly reported foreign addresses used to register multiple companies from 1 July 2014 to 30 June 2015.

trading to move the money," and suggested that the clients were not looking to profit from the trades, similar to the Moscow Mirror Network case.[17]

Given mirror trades can be used to facilitate illicit financial activity across numerous jurisdictions, the following red flags, taken together, can help financial regulators and law enforcement detect if a collection of securities trades is suspicious:

1. An entity or individual repeatedly requests unprofitable or minimally profitable purchases and/or sales of securities.

2. An entity or individual exclusively requests securities trades in one direction, i.e. buy only or sell only.

3. An entity with shell company-like characteristics requests the sale and/or purchase of securities.

4. An entity shares ownership with other entities requesting similar securities trades or with securities brokerages acting on their behalf.

5. An entity purchases securities and immediately transfers ownership of them, or an entity receives a transfer of securities and immediately sells them.

6. An entity engages in transactions that do not match its customer profile. For example, an entity requests the purchase of securities in oil and gas, even though its customer profile indicates that it is engaged in the trading of textiles.

7. An entity engages in disparate activities, one of which is securities trading. Other activities commonly include the import or export of textiles, electronics, and/or building materials.

FinCEN will continue working with domestic and foreign regulators and regulated entities to understand the scope of this issue and determine to what extent additional awareness of the problem is needed.

Source Note

FinCEN's knowledge of the mirror trading method is primarily derived from information about the Moscow Mirror Network. We relied on the following sources for this Intelligence Assessment:

- Open source reporting, including *Bloomberg, the New Yorker,* and Russian press, for confirmation of the methodology.

- Sensitive financial information obtained by FinCEN, which was useful for establishing transactional relations, ownership information, and reported locations of the Network entities.
- Deutsche Bank, which provided information into how its services were used by the Network to facilitate the securities trades, and individuals and entities involved in the activities.
- A foreign government, which provided information regarding a European bank's role in mirror trading and information about related entities that held bank accounts there.

Note: FinCEN encourages all law enforcement agencies that have equities in the subject(s) of this FinCEN Intelligence Assessment to de-conflict case sensitive information and network.

Please contact the FinCEN Production Management Office [redacted] ***if you have any questions pertaining to this report. Reference Report*** [redacted] ***and*** [redacted].

NOTE: This survey can only be accessed using Internet Explorer or Google Chrome browsers.

Warning Regarding Use And Dissemination

The information in this document is to be used for lead or investigative purposes only. The information may not be released, disseminated, disclosed, or transmitted outside your organization, or in particular used as evidentiary material or presented in court or other formal proceedings, without the prior, written approval of the Financial Crimes Enforcement Network (FinCEN). This document contains information that is protected from unauthorized disclosure by the U.S. Bank Secrecy Act (BSA) and other laws, as well as the Egmont Group Charter. Unauthorized release of information contained in this document is unlawful and may result in penalties including the loss of access to information.

[1] http://www.bloomberg.com/news/articles/2016-03-15/russia-arrest-said-to-be-linked-to-deutsche-bank-trading-probe, retrieved 3 November 2016.
[2] Promsberbank Inventory Report.
[3] BSA IDs [redacted] and [redacted], and foreign government source.
[4] http://www.newyorker.com/magazine/2016/08/29/deutsche-banks-10-billion-scandal, retrieved 6 October 2016.
[5] BSA IDs [redacted], [redacted], and [redacted].
[6] http://www.intellinews.com/russian-cb-pulls-brokerage-license-amid-deutsche-bank-scandal-89232/, retrieved 29 November 2016.
[7] http://www.cbr.ru/eng/press/pr.aspx?file=06072015_162647eng2015-07-06T16_22_34.htm, retrieved 3 November 2016.
[8] BSA ID [redacted].
[9] http://www.newyorker.com/magazine/2016/08/29/deutsche-banks-10-billion-scandal, retrieved 6 October 2016.
[10] https://www.treasury.gov/press-center/press-releases/Pages/jl0574.aspx, retrieved 1 November 2016.
[11] http://www.latimes.com/local/la-me-payroll-theft-20140211-story.html, retrieved 13 October 2016.
[12] BSA ID [redacted] and supporting documentation.
[13] https://www.treasury.gov/press-center/press-releases/Pages/jl2196.aspx, retrieved on 13 October 2016.
[14] BSA ID [redacted].
[15] Sensitive law enforcement information.
[16] *The Board of Directors of Chicago Board Options Exchange, Incorporated,* Decision No. 14 BD 01, File No. 11-0009, date 29 October 2014.
[17] *Ibid.*, p. 14.