TRANSPARENCY INTERNATIONAL RUSSIA

UNRAVELING THE WEB

MONEY LAUNDERING THROUGH E–PAYMENTS FROM RUSSIA TO THE UK

TRANSPARENCY INTERNATIONAL RUSSIA

2024

Transparency International Russia is an integral part of the global Transparency International movement, committed to combating corruption and promoting transparency and accountability worldwide. Our efforts include conducting thorough research, publishing detailed reports, and collaborating with various partners to expose and address corruption in all its forms.

Since March 2022, we have been operating in exile due to Russia's repressive regime and stringent war censorship. Despite these significant challenges, we remain unwavering in our dedication to the principles of freedom and openness. We continue to advocate for a future where governments are transparent and accountable, free from corruption and injustice. We believe that, through collective effort, we can build a society where power is exercised with integrity and in the best interest of the people.

Our mission is to combat corruption and uphold the values of transparency, accountability, integrity, and honesty. We aspire to create a world free of corruption, and together, we will achieve this goal.

ACKNOWLEDGEMENTS

Report written by:
Kristine Baghdasaryan

Research by:
Kristine Baghdasaryan

Review by:
Ilia Shumanov

Legal review:
G M

Editor:
Grigorii Slobodzian

We are grateful for the support and assistance
of Steve Goodrich, Ben Cowdock Transparency International UK
Dmitrijus Apockinas PSP Lab LLP

This Report was edited and updated on 24 September 2024

LIST OF ABBREVIATIONS

- AML - Anti-Money Laundering
- API - Authorized Payment Institution
- APP - Authorized Push Payment
- CFD - Contracts For Difference
- CZK - Czech Koruna
- DAML - Defence Against Money Laundering
- EEA - European Economic Area
- EMI - E-money Institutions
- EMD - Electronic Money Directive
- EU - European Union
- FATF - Financial Action Task Force
- FCA - Financial Conduct Authority
- FX - Foreign Exchange
- GVA - Global Venture Alliance
- ML - Money Laundering
- NCA - National Crime Agency
- PEPs - Politically Exposed Persons
- PI - Payment Institutions
- TF - Terrorist Financing
- UBO - Ultimate Bene icial Owner
- UK - The United Kingdom of Great Britain and Northern Ireland
- USD - United States Dollar

TABLE OF CONTENTS

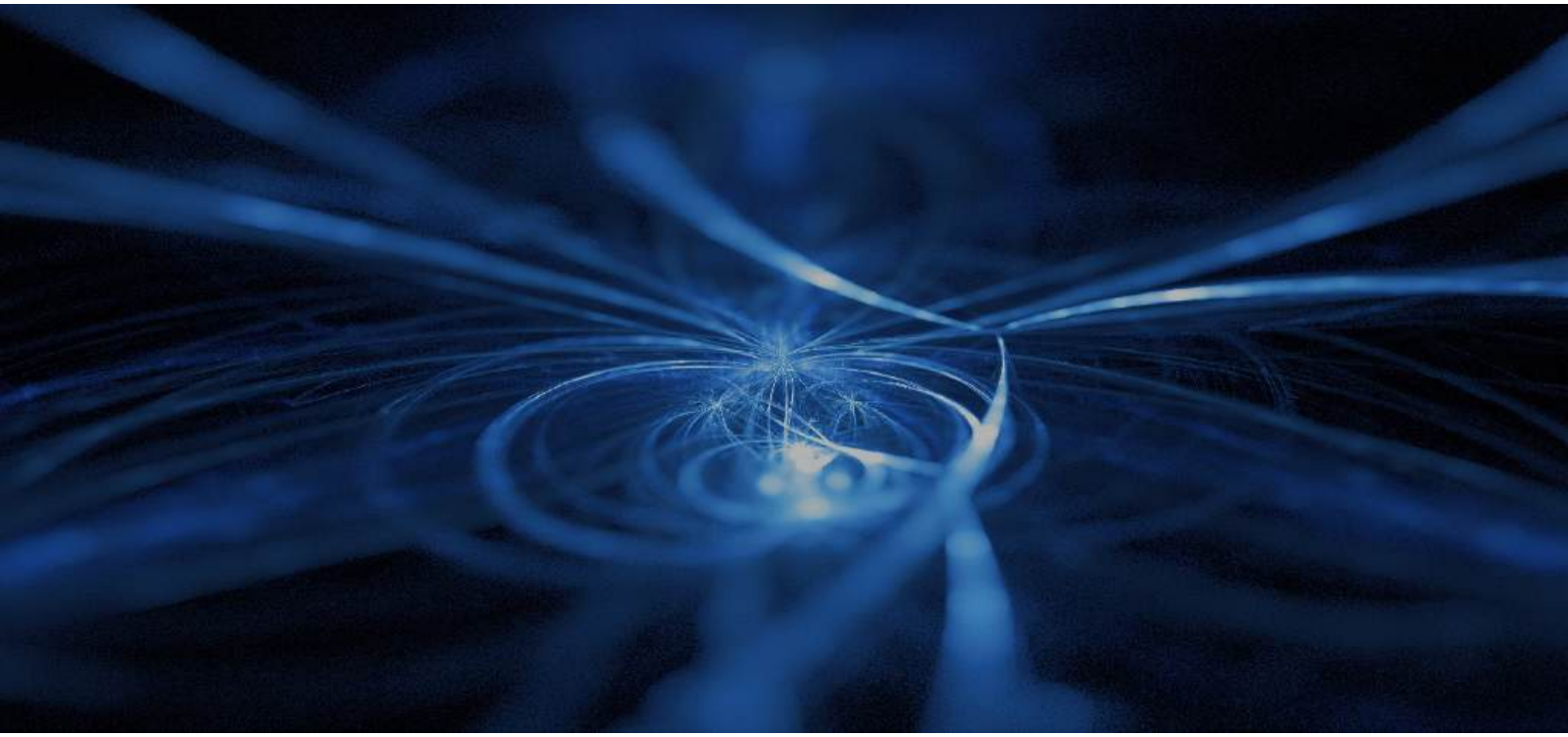
EXECUTIVE SUMMARY

In our previous research, *Anonymity for sale: the thriving black market of crypto-to-fiat mules*[1], we explored the clandestine use of cryptocurrency for transferring funds across borders undetected. We highlighted a dark market where anonymous personal crypto-to-fiat bank accounts functioned as money mules within the digital domain. These legitimate fiat bank accounts were linked to fictitious identities and used to launder money under the guise of legitimate transactions.

In a new investigation, Transparency International Russia focuses on a potentially more dangerous avenue: the trade of e-payment systems accounts for legal entities. Unlike personal accounts, these business accounts are not subject to the same transaction amount limits, posing a far greater risk for the uncontrolled movement of large sums of money. Our research indicates an illegal black market for these accounts on the dark web platforms with fabricated identities, offering criminals an ability to obscure large-scale financial transfers from scrutiny.

We look at the alarming ease with which these business accounts are trafficked on the Russian speaking dark web platforms. Frequently sold as accounts of European and UK citizens under the guise of legitimate entities, these business accounts become the perfect vehicles for laundering large sums of money under the radar. Our findings raise serious questions about how UK payment service providers are responding to these risks, and whether more can be done to shut down these avenues for cross-border illicit financial flows. They also query whether the FCA has taken too much of a permissive approach to authorizing and supervising this regulated community in the rush to lower red tape for this emerging market.

This research was initiated to highlight risks of money laundering activities, particularly involving Russian stakeholders (individuals, companies), who can exploit the vulnerabilities in these e-payment systems. Russia's extensive network of PEPs, businessmen, and criminal organizations could easily use these vulnerabilities to launder money on a large scale, impacting the financial integrity of both European and global markets. By shedding light on these practices, we aim to enhance the understanding of the risks and promote more effective regulatory and enforcement actions to mitigate these issues. This research underscores the necessity for a focused approach to combating Russian-linked money wlaundering activities within the e-payment sector.



KEY POINTS:

By highlighting these widespread issues through detailed case studies, we aim to foster a better understanding of the risks and drive more effective regulatory and enforcement actions. We intend to showcase common problems within the e-payment sector and to illustrate these with specific examples to underline the importance of addressing these red flags to enhance overall financial security. This comprehensive approach not only captures the complexity of the issue but also helps gather knowledge and resources to address financial crime in the digital age.

Regulatory Gaps and Sophistication of Money Laundering:
Despite stringent AML procedures in place, money laundering activities within the e-payment sector have persisted and become increasingly sophisticated. This paradox underscores significant regulatory gaps and requires more rigorous enforcement and oversight mechanisms.

High-Risk Profiles and Regulatory Challenges: The report identifies several e-payment platforms, such as Payrow, Paysend, ANNA Business, and Gemba Finance, that have significant vulnerabilities for money laundering. These platforms often operate through complex corporate structures and offshore entities, which obscure true ownership and can facilitate illicit financial flows. The involvement of politically exposed persons (PEPs) and high-risk connections further exacerbates the risk.

Role of the Dark Web and Illicit Markets: The research reveals a thriving market on the dark web where verified business accounts are bought and sold with ease. These accounts, often registered under false identities using genuine identification documents, enable large-scale money laundering operations. The dark web provides a secretive avenue for illegal activities, including the trading of e-payment accounts designed for money laundering purposes.

International Cooperation and Regulatory Oversight: The report emphasizes the necessity for stringent regulatory controls and international cooperation to tackle the misuse of e-payment systems. Harmonizing regulatory standards and fostering closer cooperation between regulatory bodies in the UK, EU, and Russia are critical to closing loopholes exploited in e-payment systems.

BACKGROUND

Despite the FCA's authorization of more than 200 of e-payment companies in the UK since 2018 and stringent AML procedures[2] in place, money laundering activities persist with increasing sophistication and intensity. This paradox highlights a critical gap in the regulatory framework and underscores the necessity for more rigorous enforcement and oversight mechanisms.

The regulatory environment in the UK and EU has been evolving to address these challenges. In 2019 UK Government brought crypto asset exchange providers within the scope of the Money Laundering Regulations 2017, requiring them to undertake due diligence on their customers, keep adequate records, and better assess money laundering risks.[3] In 2023, they went further and legislated to limit the promotion of cryptoasset products in the UK to specific firms authorised by the FCA.[4]

To illustrate the significant money laundering challenge faced by the e-payment sector, consider the startling fact that 18% of all Defence Against Money Laundering (DAML) suspicious activity reports in the UK emanate from this relatively small sector. This statistic starkly contrasts with the sheer volume of transactions handled by the much larger conventional banking sector, highlighting a disproportionate vulnerability in e-payments. The high number of DAMLs indicates that e-payment platforms are prime targets for money launderers, posing substantial risks despite the sector's smaller scale.[5]

Imagine a scenario where a small e-payment company finds itself at the center of a regulatory storm. This company, although not as vast as traditional banks, has become a hub for suspicious activities. Each DAML submitted represents a potential brush with criminal proceedings if illicit transactions are not intercepted and reported. The definition of a DAML underscores its gravity: it pertains to transactions suspected of involving money laundering, where processing such transactions without intervention could result in the firm committing a criminal offense. This demonstrated that even if the company has nothing to do with the money laundering performed by the independent players who are using these platforms for illegal activities, the company is still the one to bear all responsibility.

This situation becomes even more pressing when we compare the sector's figures. Despite handling fewer transactions than conventional banks, the e-payment sector's substantial share of DAMLs reveals its critical role in the money laundering ecosystem. The statistics from the report of the National Crime Agency (NCA) serve as a clarion call for more stringent measures and oversight. Furthermore, the overall size of the e-money industry is significantly smaller than the conventional banking sector, as evidenced by data from the FCA, which further emphasizes the disproportionate risk.[6,7]

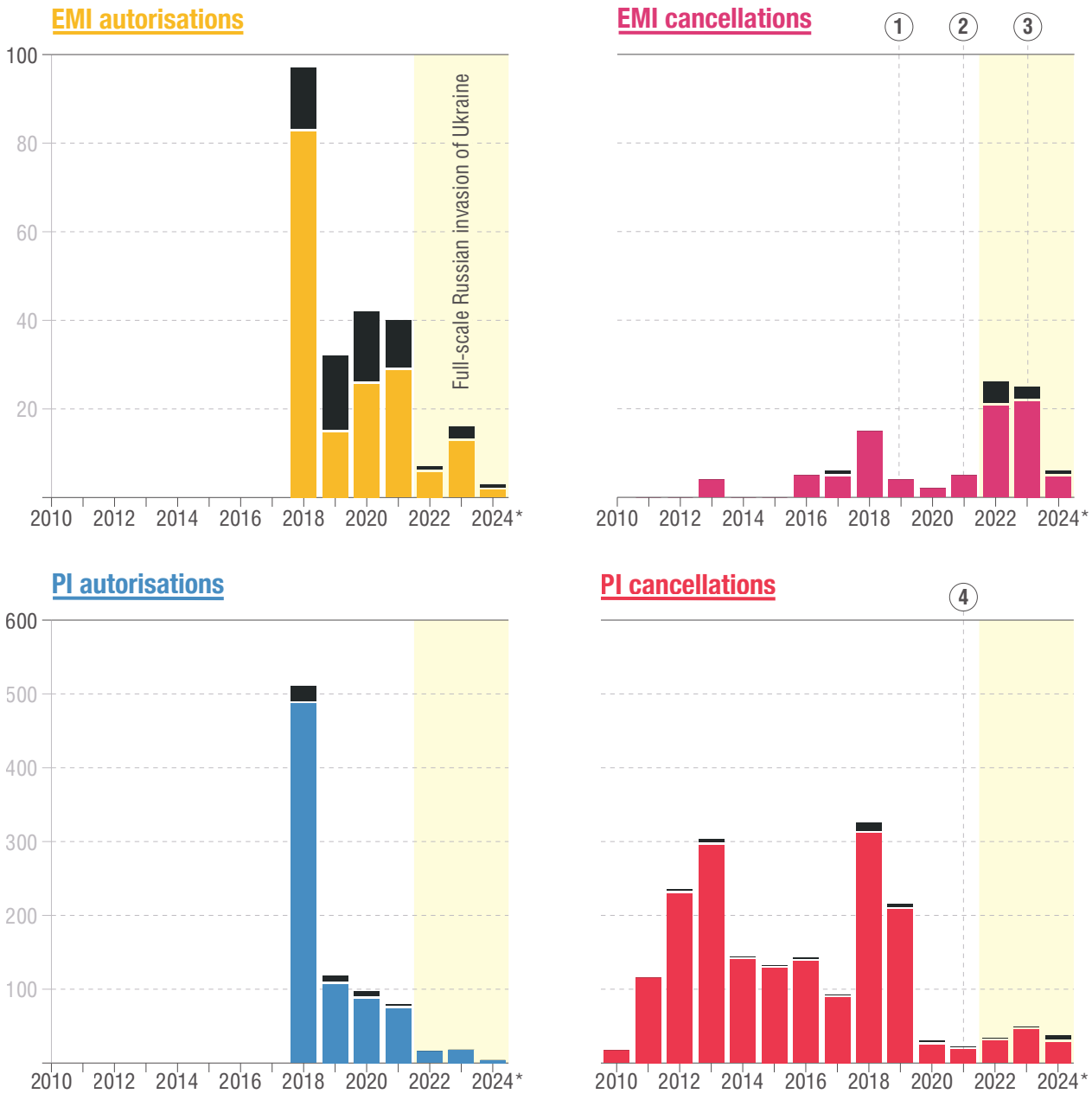
In theory, the new regulations have helped to reduce the risk posed by crypto firms by requiring them to comply with AML rules. They are now subject to similar Know Your Customer requirements and cannot advertise products in the UK without some form of authorisation. However, in practice, what we are seeing is high risk activity still going through these firms - risks compounded by some of their questionable ownership structures.

In conclusion, the high incidence of DAMLs in the e-payment sector, despite its smaller size, underscores the urgent need for robust regulatory frameworks and enhanced international cooperation. This evolving regulatory landscape is crucial in safeguarding e-payment systems from being misused for money laundering, reflecting a broader commitment to financial integrity and security.

The latest research by PSP[8] Lab provides statistics on the number of E-money Institutions (EMI) and Payment Institutions (PI) licenses issued, as well as those that have been withdrawn or canceled, within both the EEA and the UK in the period of 2018-2023 shows a sharp rise in EMI **license withdrawals and cancellations**. As shown in the figure below, this trend coincided with several scandals in banking, payments, and e-money that stained the sector's reputation, leading regulators to adopt a more stringent approach to the authorizations and supervision of PSPs. Prominent cases include Wirecard (German bank), Railsr (Lithuanian EMI), Transactive Systems (UK EMI), Viola Money (UK EMI), ePayments (UK EMI), and Premier FX (UK PI). Recently, the European Banking Authority published a report[9] on money laundering (ML) and terrorist financing (TF) risks associated with payment institutions.

Number of EMI and PI Authorisations and Cancellations in the UK

Including Companies Related to Russia



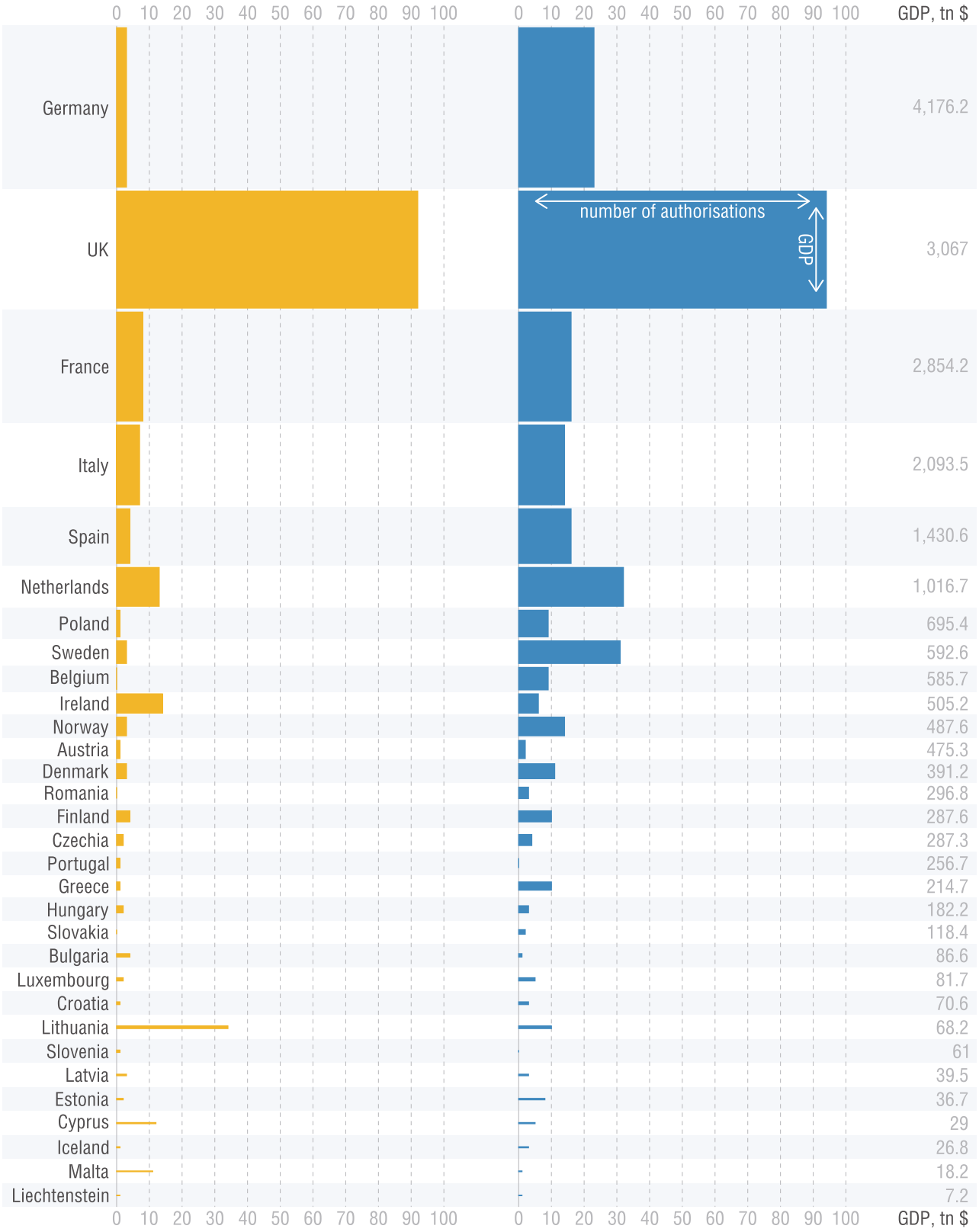
1 — ePayments Systems (UK EMI)
2 — Transactive Systems (UK EMI), Viola Money (UK EMI)
3 — Railsr (Lithuanian EMI)
4 — Premier FX (UK PI)

*Data as of April 2024
The margin of error did not exceed 4%
Source: EUCLID database, FCA Register. Accessed 15.12.2023, World Bank

It's also worth mentioning that since 2018 a shift in new authorisations can be detected from the UK to jurisdictions with friendlier regulations and the ability to provide access to the EEA, such as Ireland, Netherlands, Malta, Latvia, and Spain. Among these, Lithuania, Latvia, Cyprus, and Malta attract EMI and PI entrepreneurs to a degree disproportionate to the size of their domestic economies.[10]

Number of Authorisations of EMIs and PIs Granted in the EEA and UK from 2020 to 2024

Showing the Relationship Between the Number of Authorizations and GDP*



*GDP (current US$) as of 28.06.2024, average GDP for 2020–2024
Source: EUCLID database, FCA Register. Accessed 15.12.2023, World Bank

Our findings are further underscored by insights from the October 2023 Authorised Push Payment (APP) Fraud Performance Report, which reveals significant ongoing challenges in managing APP fraud, a key component of financial crime.[11] It discusses the most comprehensive data on the scale and impact of APP fraud published to date, covering 95% of Faster Payments System in the UK by value and volume. The report emphasizes the need for improved outcomes for victims and the introduction of a new reimbursement requirement in 2024, which is expected to drive significant improvements in fraud prevention and victim compensation.[12]

The urgency of addressing money laundering in e-payment systems, particularly in the UK and EU, is further underscored by insights from the Together in Electric Schemes report by Transparency International UK.[13] This report delves into the vulnerabilities of EMIs in the UK, highlighting how these platforms can be misused for illicit financial activities. It emphasizes the need for stringent regulatory oversight and robust enforcement mechanisms to combat money laundering risks in this sector. Incorporating the findings and recommendations of this report is crucial in understanding the broader context of e-payment vulnerabilities, enhancing our analysis of regulatory actions, and formulating effective strategies to safeguard against financial crimes in digital financial services.

When conducting our comprehensive analysis of money laundering in e-payment systems, we discovered the proactive approach taken by companies like Wirex in enhancing their security measures. Wirex's initiative against dark web activities and money mules represents a significant step in the industry's effort to combat financial crimes. This development showcases the effectiveness of implementing robust security protocols in e-payment platforms, aligning with our recommendations for heightened vigilance and technological advancements to safeguard financial transactions.

Methodology

This report aims to illuminate critical vulnerabilities within the e-payment sector by urging a reassessment of current AML strategies and the implementation of more robust monitoring systems to prevent the integration of illicit funds into the mainstream financial system. To achieve this, we conducted a detailed analysis using specific case studies to highlight widespread issues and common red flags in the industry.

Our methodology involved the following steps:

EXTENSIVE REVIEW OF PUBLICLY AVAILABLE INFORMATION:

We examined a wide range of publicly available documents, including financial statements, regulatory filings, and industry reports. This helped us gather baseline data on the operations, ownership structures, and compliance histories of various e-payment platforms.

CASE STUDY ANALYSIS:

We selected specific e-payment platforms such as Payrow, Paysend, ANNA Business, and Gemba Finance, among others, to serve as detailed examples. These companies were chosen to illustrate typical vulnerabilities and red flags prevalent across the sector. By examining these platforms, we aim to demonstrate how common issues manifest in real-world scenarios, providing concrete evidence to support our findings.

RESEARCH INTO DARK WEB MARKETPLACES:

Our research included an exploration of dark web marketplaces where verified business accounts are bought and sold. This research provided insights into the

methods used by criminals to exploit these accounts for money laundering purposes. The information gathered from these marketplaces was crucial in understanding the scale and complexity of the problem.

INTERVIEWS AND STAKEHOLDER ENGAGEMENT:

We conducted undercover interviews with sellers of e-payment accounts and spoke with industry stakeholders to gain deeper insights into the operational tactics of illicit traders and the challenges faced by legitimate businesses. These interviews helped us validate our findings and provided additional context for our case studies.

COMPARATIVE ANALYSIS OF REGULATORY FRAMEWORKS:

We analyzed the regulatory environments in the UK, EU, and other relevant jurisdictions to identify gaps and inconsistencies in AML enforcement. This analysis highlighted the need for harmonized regulatory standards and closer international cooperation to tackle the misuse of e-payment systems effectively.

Patterns

Patterns of abuse in e-payment systems were identified, highlighting how lax AML controls are, lack of proper customer due diligence, and the use of cryptocurrency-to-fiat conversion services create avenues for laundering money.

Case studies reveal instances where e-payment systems could be exploited by actors seeking to launder money from Russia to the UK, often through the use of e-payments and money mules.

IN-DEPTH ANALYSIS OF RED FLAGS WITH CASE STUDY EXAMPLES

In our report on money laundering through e-payment systems, particularly in connection with the UK, EU, and Russia, we identify and elaborate on several critical red flags. Each red flag is paired with specific examples from our research, providing practical insight into how these indicators can signal potential illicit activities.

These red flags serve as crucial indicators for law enforcement and regulatory bodies to identify and investigate potential money laundering operations effectively. By providing concrete examples from our research, we aim to underline the practical applications of these red flags in real-world scenarios, assisting stakeholders in crafting targeted interventions to combat financial crimes in the e-payment sector.

1. Politically Exposed Persons (PEPs) and High-risk Connections

Involvement of PEPs and their close associates, especially those linked to significant corporations or political entities, requires enhanced due diligence due to the risk of money laundering. Despite these requirements being mandated by FATF recommendations, deficiencies in enforcement have been observed. Previously identified AML violations identified by the Czech National Bank in a Czech electronic payment company associated with a PEP from Gazprom raise additional suspicions about the risks of money laundering in a UK e-payment company, where Gazprom PEP was a shareholder.

2. Compliance and Regulatory Issues and High-risk Jurisdictions

Issues with adherence to regulatory standards, particularly in emergent e-payment platforms, highlight potential vulnerabilities exploitable for money laundering activities. Research into Payrow, a newly established e-payment service, showed repeated failures in meeting regulatory compliance requirements

in Lithuania, coupled with suspicious transaction patterns indicative of risk of money laundering. Despite these regulatory challenges and the revocation of the licenses in Lithuania, some of the e-payment operators can continue to operate successfully in other countries, illustrating a significant issue where e-payment platforms can face sanctions in one jurisdiction but relocate and thrive in another. This mobility highlights the need for international cooperation in regulatory oversight to prevent such platforms from escaping legal consequences.

3. Opaque and Complex Corporate Structures

The use of intricate corporate structures and complex entities often obscures true ownership and facilitates money laundering. Our research into e-payment platforms revealed their involvement in a complex network of opaque entities in Cyprus, Malta, and Russia, making it challenging to trace the ultimate beneficial owners. Transactions exhibited unusual patterns, such as high-frequency transfers and round-number transactions, indicating possible layering strategies. This lack of transparency and complexity in corporate structure underscores the need for regulatory scrutiny and robust AML measures to address such risks.

In our ongoing efforts to unravel the complex networks of money laundering that exploit electronic payment systems, we have grounded our research in detailed investigations originating from dark web marketplaces. These platforms, often hidden from the conventional Internet, provide a secretive avenue for illegal activities, including the trading of verified e-payment accounts designed for money laundering purposes.

Dark Web Research Methodology

Our approach involved a systematic exploration of the dark web to understand how e-payment accounts are marketed and sold. Transparency International Russia conducted an investigative study aimed at purchasing Gemba Finance, Paysend, ANNA Business, and Payrow accounts registered under stolen or fabricated identities. These accounts serve a critical role in money laundering: they allow transactions to be made without financial institutions knowing the true identities of the account holders, effectively acting as money mules.

Investigative Steps Taken

VENDOR CONTACT:

We engaged with several sellers on dark web platforms to probe the terms and conditions of their services. This direct interaction helped us gather insights into the operational tactics of these illicit traders.

UNDERSTANDING THE MARKET:

Our conversations revealed a disturbing ease of acquisition and a broad range of prices, reflecting the accessibility and scale of this underground market. Prices ranged from USD 150 for personal accounts to USD 1000-1800 for business accounts.

GEOGRAPHIC SPREAD:

The accounts for sale originated from Eastern Europe, particularly Latvia, Estonia, Czech Republic, and the UK. This geographic information points to specific regions as hotspots for this type of financial fraud.

VERIFICATION AND ANONYMITY:

Sellers claimed that all accounts were registered using genuine identification documents, which could be further authenticated by photos or videos to pass additional verifications by financial platforms like Gemba Finance, Paysend, Payrow, ANNA Business.

IMPLICATIONS FOR CASE STUDIES:

Given that all the e-payment platforms explored in our report were identified through this dark web research, our case studies will focus on these platforms to illustrate broader patterns and strategies used in digital money laundering. This focus allows us to:

HIGHLIGHT SPECIFIC RISKS:

By detailing the operations and vulnerabilities associated with each e-payment system identified through the dark web, we can demonstrate specific risks and suggest targeted interventions.

EDUCATE STAKEHOLDERS:

Providing concrete examples from our dark web findings helps in educating financial institutions, regulators, and the public about the sophisticated methods used by launderers, thus enhancing preventive measures.

ADVOCATE FOR ROBUST CONTROLS:

Our research underscores the necessity for stringent regulatory controls and international cooperation to tackle the misuse of e-payment systems for money laundering.

CROSS-JURISDICTIONAL COOPERATION:

Foster closer cooperation between regulatory bodies in the UK and EU to facilitate the exchange of information on suspected money laundering activities and harmonize regulatory standards to close loopholes exploited in e-payment systems.
Sector-Specific Guidelines and Reporting Mechanisms: Create detailed guidelines for the e-payment sector on identifying and reporting suspected money laundering activities, including specific indicators of illicit use of cryptocurrency and e-payment systems accounts for legal entities within these platforms.

Purchasing accounts registered with a money mule

We examined the possibility of purchasing a Paysend, Gemba Finance, ANNA Business, and Payrow business accounts registered with someone else's identity, who would act as a money mule — allowing payments to be made without the e-payment systems knowing the true identity of those really moving the money. In order to get knowledge of how the market works, we contacted seven sellers to understand the conditions on which they offer their services and prices. Although buying a verified account is illegal, we found it to be a simple procedure. Based on our correspondence with the sellers, we found that the accounts were registered in the names of citizens of Latvia, Estonia, and the UK. The sellers offered accounts registered in several countries in Europe: Bulgaria, Poland, Spain, Italy, France, Ukraine, and the UK.

The price varied from USD 150 for a personal account to USD 1000-1800 for a business account. The most widespread was the offer of accounts for sale registered in the Baltic states, such as Latvia and Estonia. Each seller stated that original identification documents were used for registration.

A SAMPLE ADVERTISEMENT OFFERING VERIFIED ACCOUNTS FOR SALE IN DIFFERENT SYSTEMS

HOT
Svumup business uk
Worldfirst busienss
Pockit personal
Monzo business nox
Payrow business UK
Gemba Business UK
G2A business UK 0
Kraken business uk
Payset business UK
Bunq personal
Revolut personal IT ES BG PL
Wise business uk

Telegram support: @AUTOMATIC_SUPPORT
CHANNEL https://t.me/joinchat/S0PjwbfRw
bfRwzZkFmPI

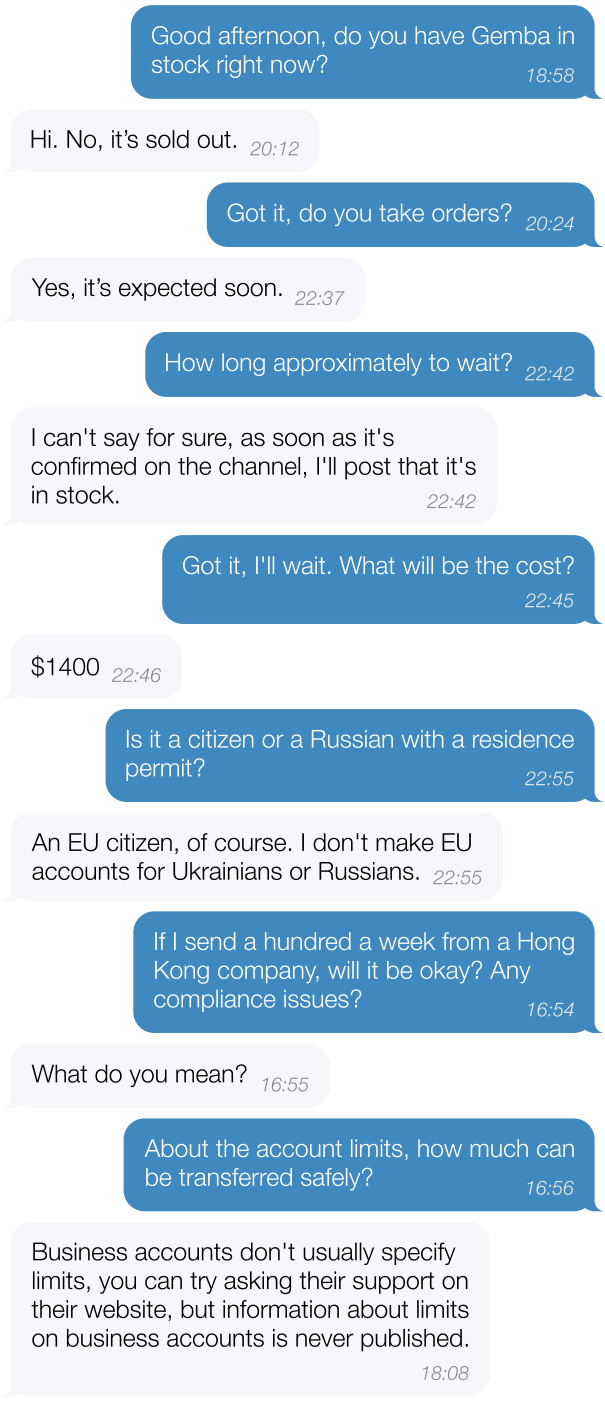
17:21

POLITICALLY EXPOSED PERSONS (PEPS) AND HIGH-RISK CONNECTIONS

The involvement of PEPs in Gemba Finance, Paysend, and their affiliated entities raises significant red flags due to the heightened risk of money laundering. Our investigation highlights the participation of high-profile individuals who have extensive connections to influential political and economic networks in Russia. Some of them are linked to major Russian state companies, intensifying concerns about the company's compliance with international regulations and the potential for illicit financial activities. We have found that business accounts of Gemba Finance and Paysend are available for purchase on the dark market, raising a significant concern and presenting an opportunity for potential money laundering activities.

UK-based company Gemba Finance, established in Oct 2017, has been granted FCA authorization to conduct payment services activities as an Authorized Payment Institution (API) from 13 March 2019. Gemba is an online transactional banking service for startups and financial services to embed transactional banking functionality into their apps or services.

We have identified Russian citizen Alexander Legoshin, UBO of Gemba Finance, and Vladimir Derevyagin, a Russian citizen with a UK residency[14] and an Israeli citizenship, a director of the company since 2019. During 2019-2022 the shares of the company were allocated between three shareholders: Alexander Legoshin, Vladimir Derevyagin, and **Evgeny Zemlyanoy**.[15]



Chat with Bull Frog, offering the sale of Gemba Finance accounts

Alexander Legoshin purchased financial service company Paymaster AS in 2017[16] as sole shareholder through his Hong Kong based Metropolitan International Group Limited. Paymaster AS registered in Prague in 2017. Since 2021, Evgeny Zemlyanoy has been one of the owners of Paymaster AS, and since 2023, according to the court

registry of the Czech Republic, he has been a shareholder of Paymaster AS.[17]

Paymaster is the owner of the trademark Saufi AI, Cryptocurrency payments firm Saifu, which is licensed by the Czech National Bank. According to information from social media, Legoshin is one of the company owners. Based on social media information, the official website Saufi A has been frozen since 2020.

In 2019, the Czech National Bank initiated administrative proceedings against Paymaster AS due to multiple violations, including AML violations:

- Incorrect reporting of payment transaction volumes in 2018, including significant underreporting in one quarter and overreporting in another.

- Breach of fund separation rules: On January 22, 2019, Paymaster transferred its own funds to a client's account designated for client funds entrusted for payment transactions and kept its own funds there until at least February 8, 2019.

- Failure to provide pre-contractual information to clients in multiple instances in 2018 and 2019.

AML compliance breaches included inadequate identification of clients and PEPs, lack of proper risk assessments and controls for money laundering and terrorist financing risks, and failure to conduct due diligence on clients.

The Czech National Bank revoked Paymaster's license to operate as a small-scale payment service provider, citing serious violations of the Payment System Act and AML legislation, and fined Paymaster 1 million CZK (approximately 43,250 USD) for these breaches.

This decision underscores the necessity for financial institutions, especially those offering e-payment services, to maintain rigorous compliance frameworks to prevent money laundering and terrorist financing, and to adhere to operational regulations strictly.

We conducted interviews with Legoshin and Derevyagin. Despite Legoshin's claim that they are now heavily engaged in AML compliance, Gemba's accounts for legal entities could be purchased on the dark market. Legoshin admits that Gemba did not perform PEP checks on Zemlyanoy, which is unusual for someone who asserts to be actively engaged in anti-money laundering practices. Regarding Zemlyanoy and his connection to Gazprom, they denied any involvement, although official records still list Zemlyanoy as part of Paymaster. Derevyagin claimed he had long ceased any active roles and had transferred all his shares to Legoshin, yet later admitted he still holds a percentage in Gemba but does not make any decisions.

Furthermore, Legoshin initially denied[18] any connection between Gemba and Paymaster but later mentioned plans to merge the two companies through Gemba Luxembourg for administrative purposes, which did not materialize.

Paysend's connections to PEPs extend significantly through its ownership and strategic relationships, highlighting potential risks in compliance with anti-money laundering regulations. Our findings demonstrate that this is not unique to Paysend.

Elvira Abdulkerimova, along with her husband Abdul Abdulkerimov, are identified as the UBOs of Paysend Group Limited.

Abdul Abdulkerimov originates from the Republic of Dagestan and holds Russian, Cypriot, and British citizenships, according to Companies House filings. Abdulkerimov is a business partner with Magomed Musaev[19], a family member of Russian PEP

whose father-in-law is the former Head of the Russian Republic of Dagestan, Ramazan Abdulatipov. [20]

Magomed Musaev [21] is the President of Global Venture Alliance (GVA) [22], a venture capital investment firm founded by Musaev, Abdulkerimov, and Pavel Cherkashin in 2011. [23] GVA provided initial capital for Paysend [24] and remains a significant shareholder of Paysend Group. [25]

Musaev is affiliated with Paysend, serving as president of Paysend's shareholder GVA. He assisted Dagestani billionaires, including sanctioned Russian oligarch Suleiman Kerimov, in setting themselves up in the US. Kerimov invested in GVA through Prosperity Investments, based in Guernsey.

The Abdulkerimovs are also connected to Russian PEPs through Ozerna LLC [26], a Russian-based company where Elvira Abdulkerimova held 50% of the shares until 2023.

While it remains uncertain whether Paysend directly provides services to politically connected or sanctioned Russian individuals, the close associations and business relationships they maintain with such figures significantly increase the risk. Similarly, although the exact nature of Ponomarenko's financial involvement with Paysend is not fully known, the Ponomarenko family history of complex international money transfers, as seen with Finaport, suggests a tendency to use financial services offering opacity and flexibility. The convergence of their past financial maneuvers and Paysend's advanced digital services presents a potential risk for misuse, highlighting the need for robust regulatory scrutiny and proactive due diligence to prevent illicit actions.

Summary of Risks Identified in Cases:

In the case of Gemba Finance, the involvement of Evgeny Zemlyanoy, a Deputy General Director at Gazprom Energoholding, highlights the risks associated with PEPs. Zemlyanoy's connections to Gazprom raise significant compliance concerns. The company's association with high-profile individuals complicates regulatory oversight and underscores the need for stringent due diligence to prevent potential money laundering.

Gemba Finance responded that they are aware of the risks associated with the sale of business bank accounts on dark marketplaces. They claim to have implemented security measures, monitoring systems, and due diligence processes to prevent such occurrences. They also claim to conduct regular audits to comply with AML regulations and collaborate with law enforcement and other financial institutions to detect and prevent illicit activities.
Gemba Finance claims Evgeny Zemlyanoy is not currently involved with their business; that Paymaster AS' regulatory failures are unrelated to their operations; and that Paymaster AS has not been related to Alexander Legoshin for some time. However, we believe that Legoshin and Zemlyanoy were involved with both Gemba

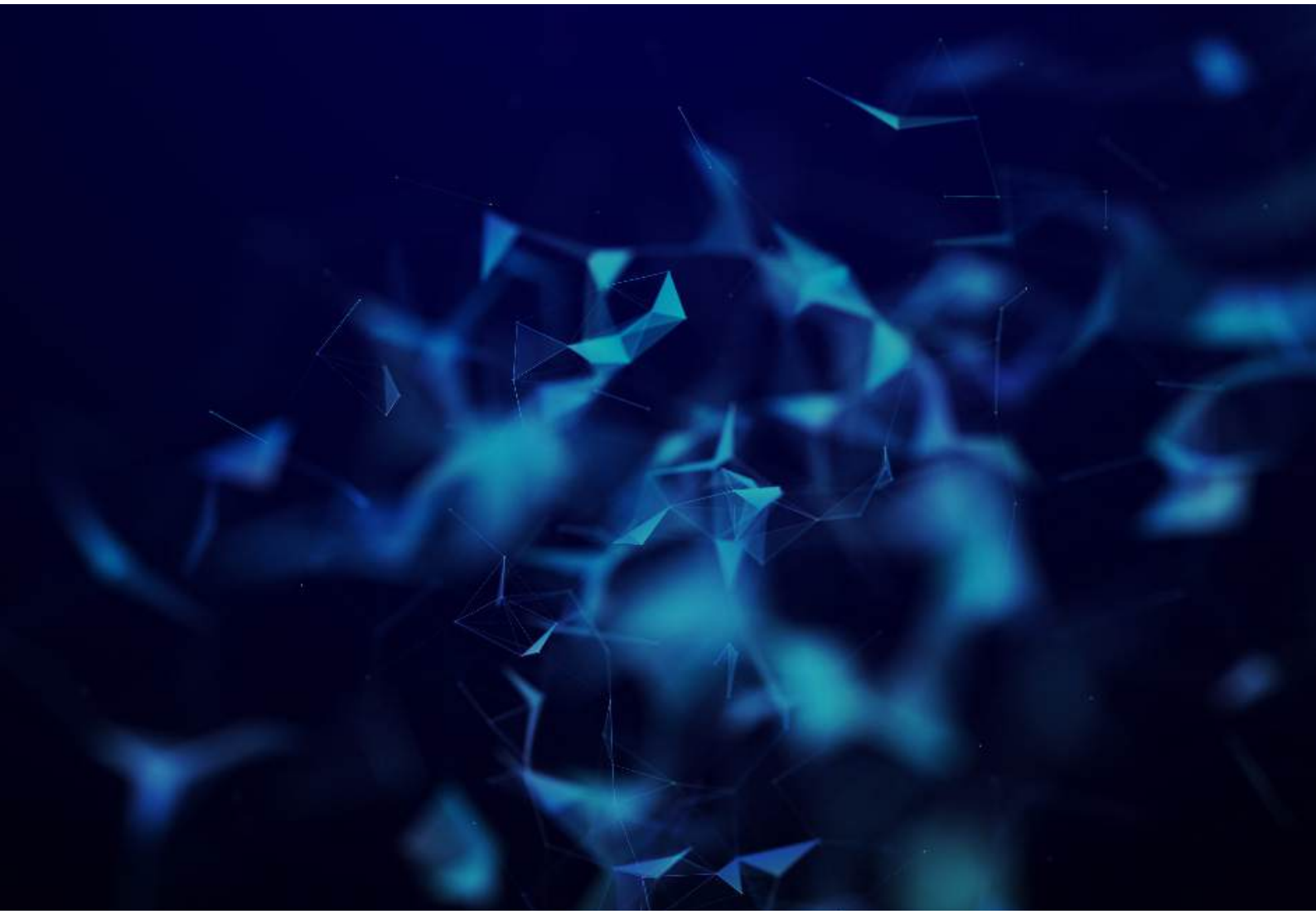
Finance and Paymaster AS simultaneously, suggesting that regulatory decisions in the Czech Republic could also impact the UK company. Therefore, any regulatory failures or shortcomings in Paymaster AS could potentially affect the reputation and regulatory obligations of Gemba Finance in the UK.

Gemba cited FCA guidelines that for persons to be considered as PEPs (politically exposed persons), they should "hold truly prominent positions and [should] not apply the definition to local government, more junior members of the senior civil service, or anyone other than the most senior military officials". This could imply that Evgeny Zemlyanoy has been classified as a low-risk PEP, as his position as a deputy director of a Gazprom Energoholding does not constitute a high-risk role due to the lack of executive power. However, in our

opinion FCA expects [27] firms to understand the nature of the positions held by PEPs and assess the risk of large-scale abuse of position accordingly. In high-risk countries, even mid-ranking officials could potentially be involved in significant corruption. Russia ranks low on the Corruption Perceptions Index (CPI) [28] since 2012 [29], further highlighting the pervasive risk of corruption. As such, the classification of Zemlyanoy as low-risk seems questionable without concrete evidence and a clear understanding of his role's potential for abuse. Therefore, while reflecting Gemba's opinion, it is crucial to highlight the necessity of thorough customer due diligence (CDD) measures given the high-risk environment and the historical context of corruption in Gazprom.

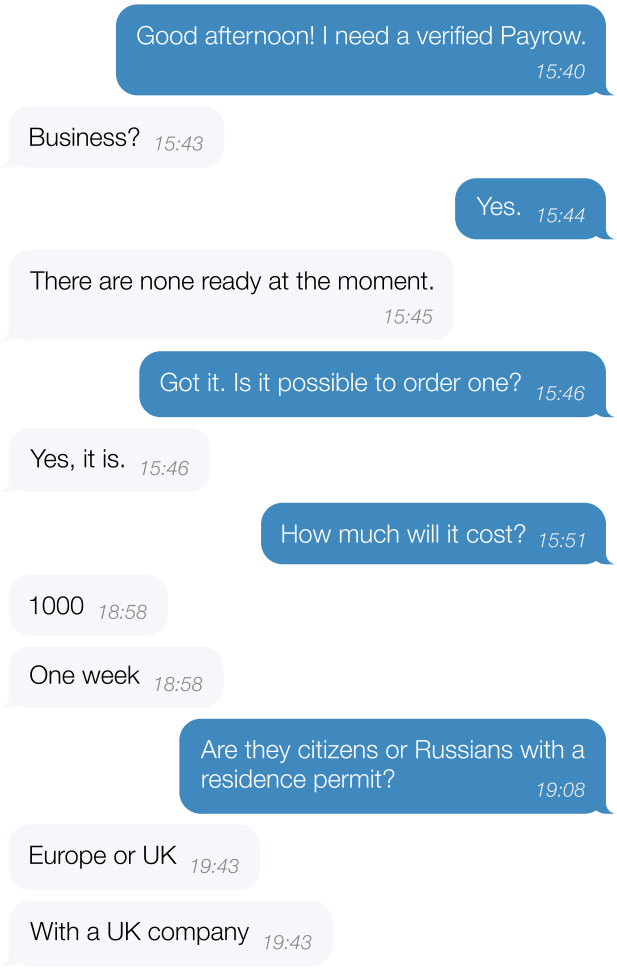
High-risk Overview:

The involvement of PEPs and their close associates in the e-payment sector presents significant risks. According to the FATF Guidance: Politically Exposed Persons (Rec 12 and 22) since PEPs are individuals who hold prominent public positions, they're at higher risk for potential involvement in money laundering and corruption. Enhanced due diligence is required when dealing with PEPs, but enforcement often falls short. The complex corporate structures and entities commonly associated with PEPs further obscure true ownership and facilitate the flow of illicit funds. These factors combined increase the risk of money laundering, as demonstrated by various cases where e-payment platforms have been exploited by politically connected individuals.



OPAQUE CORPORATE STRUCTURES AND COMPLEX ENTITIES

and complex entities to facilitate financial transactions is a hallmark of 'smurfing', designed to break down large transactions and avoid detection. Our analysis identified a network involving Cyprus and Malta front companies that were part of a complex chain of transactions stretching from Russia to the UK, designed to launder proceeds from illicit activities through multiple small transfers. As in the previously mentioned case, the dark market here represents a significant issue, facilitating money laundering and hiding illegal financial activities.



Chat with Gunna, offering the sale of Payrow accounts

Elvira Abdulkerimova (Magomedova) alongside her husband Abdul (Abdulezhil) are the ultimate beneficial owners of Paysend Group Limited incorporated in the UK in 2017. Paysend in its turn is a sole shareholder of Paysend Technology Limited and Paysend Nominees Limited.

Abdulkerimov's involvement in the financial sector began with acquiring significant stakes in Russlavbank in 2012. This acquisition initiated a series of legal and regulatory challenges, marking the start of Abdulkerimov's controversial financial and entrepreneurial trajectory.

On November 10, 2015, the Bank of Russia decided to revoke the banking license of Russlavbank. According to the regulator, the bank conducted a high-risk lending policy and failed to create adequate reserves for possible loan losses. Additionally, the bank did not comply with the legislation on combating money laundering and financing terrorism, as noted in the Central Bank's announcement.[30]

Elvira Abdulkerimova is the sole shareholder of the Cyprus-based Olnice Investments Limited. According to the 2016 financial statement of Olnice Limited, another Cypriot company, Brookstone Investment Ltd, initially provided a subordinated loan of €2,657,189 to Russlavbank. Later, Brookstone Investment Ltd sold this loan to Olnice Investment. Through a complex scheme of write-offs, the debt was never repaid.

Given the involvement of Olenice Investment Ltd, owned by Elvira Abdulkerimova, and Russlavbank, owned by Abdulkerimov, the transfer of the bank's debt raises significant anti-money laundering concerns. These

intra-family financial transactions may be attempts to manage debt obligations or minimize financial losses within the family, obscuring asset ownership transparency. This setup could facilitate money laundering by disguising asset origins or shifting liabilities to benefit family members. Additionally, these transactions may lead to conflicts of interest and attract regulatory scrutiny, necessitating thorough documentation and transparent reporting to comply with legal standards and avoid penalties.

Olenice Investment Ltd provided a large loan[31] to Paysend Holding Limited, which was then converted into shares, and also received a debt from Digital Space Ventures that was exercisable as a lender against Paysend Holding Limited. The source of funds for Olenice Investment Ltd is unclear, essentially creating Paysend by providing loans, and then conveniently forgetting about these debts, raising suspicions about the legitimacy and transparency of these financial maneuvers.

These transactions likely represent an internal financial restructuring of finances within the family's business, with concerns about transparency and the nature of the deals, hinting at possible use of complex structures for money laundering and connections to revoked licenses of QIWI and Russlavbank, highlighting risks and vulnerabilities in the financial network associated with these entities.

The financial and corporate relationships presented here suggest a tangled web of connections between Paysend, Qiwi, and entities associated with Abdulkerimov. With a focus on regulatory breaches by Qiwi Bank[32], the potential risks and impacts on its partners, including those with historical ties to Abdulkerimov, are brought to light.

Currently, Abdulkerimov operates his Russian business through UK-based Paysend Group Limited, which owns shares in the Non-banking credit organization Platezhi i raschety (a Russian e-payment firm). Paysend Group Limited also held shares in three other Russian-based companies engaged in software development until 2022: PS Development LLC, PS Processing LLC, and Robokassa LLC.[33]

Besides, Paysend is the sole shareholder of Paysend PLC, Paysend Technology Limited, and Paysend Nominees Limited (established in 2022) in the UK. According to Paysend PLC's 2022 annual report and financial statements, it has two subsidiaries engaged in finance activities in Ireland (since 2023) and in the UAE.

Summary of Risks Identified in Case:

The case of Paysend illustrates the risks associated with complex corporate structures. Paysend Holding Limited, based in Cyprus and owned by Abdul Abdulkerimov, invested in the UK Paysend Group while Olenice Investment Ltd, another entity linked to Elvira Abdulkerimova, granted a loan to Paysend Holding and later converted it into shares. The origins of the funds and the manner of debt repayment remain unclear, raising concerns about transparency and potential money laundering. Furthermore, QIWI PLC's use of Russlavbank as the settlement bank for the Contact payment system, with connections to Contact International Holding AG, underscores the challenges in tracking financial flows through layered corporate entities. Both QIWI and Russlavbank had their licenses revoked, highlighting significant risks and vulnerabilities within the financial network associated with these entities.

We have reached out to Paysend with questions about their AML policies, and their awareness of their account sales via dark markets, but no one has responded.
This complex financial maneuvering, involving multiple jurisdictions and intricate corporate setups, highlights how such structures can obscure true ownership and facilitate money laundering.

High-Risk Overview:

The use of complex corporate structures is a prevalent issue in the e-payment sector, making it challenging to trace the ultimate beneficial owners and the true origins of funds. Companies operating through multiple layers of subsidiaries and holding companies in jurisdictions with lenient regulatory environments can easily mask illicit activities. This lack of transparency allows for the layering and integration of illicit funds into the legitimate financial system. The intricate networks of these entities often span multiple countries, complicating regulatory oversight and enforcement. Such structures are frequently used to avoid detection and facilitate large-scale money laundering operations, underscoring the need for rigorous regulatory scrutiny and robust AML measures.

COMPLIANCE AND REGULATORY ISSUES

In the realm of e-payments, compliance and regulatory issues are critical red flags. These concerns arise from regulatory compliance failures, operations in jurisdictions with weak regulatory frameworks, and associations with politically exposed persons and entities involved in financial misconduct. Such factors significantly elevate the risks for financial institutions and necessitate rigorous due diligence and robust regulatory oversight.

Chat with Fantastic, offering the sale of Paysend accounts

The connections within the examined companies to entities previously involved in money laundering issues — Mercuryo, Payrnet, Sumsub — have been identified. Business accounts of Payrow, ANNA Business, available on the dark market, create a significant risk for potential money laundering activities.

Payrow Payment Systems Limited (Payrow) is authorized by the Financial Conduct Authority (FCA) (Firm reference number 903004) as an EMD Agent for PayrNet Limited. In 2023 PayrNet Limited lost its license in Lithuania. Regulators in Lithuania revoked the license of UAB Payrnet, a payments firm that was part of failed UK group Railsbank Technology Ltd., systematic and multiple violations of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions, the Law on the Prevention of Money Laundering and Terrorist Financing as well as the Law on Payments.[34] Despite these issues, PayrNet remains operational, especially in the UK, where it is listed as a subsidiary of the fintech company Railsr on its official website.[35] Although there were reports in 2023 that Railsr was facing potential bankruptcy, recent confirmations[36] indicate that the company is currently stable and performing well.

The Bank of Lithuania announced it would initiate bankruptcy proceedings against PayrNet and stated its intention to request law enforcement authorities to investigate potential criminal offenses.

PayrNet, which had a license to operate as an electronic-money institution, or EMI, across the European Union and processed some €7.5 billion ($8.3 billion) of transfers last year, violated laws linked to the prevention of money laundering.[37] It means that the institution can no longer provide financial services and has to return the funds to its clients within the set time limit.

Payrow Payment Systems Ltd was incorporated in 2019 in the UK by UK-based Skytech Solutions Group LLP

and Maltese-based Stylized Enterprises Limited[38]. According to the UK company registry, since 22.02.2024 all the shares have been transferred to a Russian national Dmitry Doykhen, resident of Switzerland who also holds a Maltese citizenship.

Another UK-based e-payment company Absolutely No Nonsense Admin Limited (ANNA Money) is a distributor of PayrNet Limited. Absolutely No Nonsense Admin Limited[39] was previously owned by the subsidiary of Mikhail Fridman's Alfa Bank. Currently, the company is owned by Boris Dyakonov and Eduard Patnellev, the founders of the Tochka bank.

Moreover, according to the latest report by Thomson Reuters, the clients of the UK-based KYC company Sumsub with tight involvement of the Kremlin and prominent Russian investors[40] are other UK-based e-payments – Mercuryo[41], Wirex, TransferGo, Unlimit, Cryptopay, Transferra UN, Inlimit. All exhibit significant compliance and security concerns. Cryptopay, previously FCA-authorized, has faced regulatory restrictions, TransferGo has been fined for AML failures in Lithuania and the UK and sanctions breaches. Inlimit's founders have complex citizenship histories and associations with firms flagged by the FCA, raising compliance issues. Clear Junction has the highest APP fraud rates among smaller banks and payment firms and has been fined for transactions with a sanctioned Russian bank.[42]

It's worth noting that Transferra UN Limited another client of Sumsub[43] incorporated in 2020 is owned by Dmitry Doykhen and Nikolay Kutuzov, previously occurring in Payrow.

Two Latvian citizens Luize Berzina and Viktors Kazankis operate as directors in Transferra UN and another e-payments company Monetley LTD which is fully owned by Cyprus Mrcr Holdings Ltd. MRCR Holdings also controls Russian-controlled crypto payment processor Mercuryo.

Two individuals are currently directors of the Payrow Payment System – Dmitry Likhno (since 2019) and Valeriy Matveev (since 2022). Dmitry Likhno has Estonian citizenship and according to the official corporate registry is a UK resident while Valery Matveev has a Dutch residence.

Lihno has a significant presence in various e-payment and cryptocurrency companies in Estonia. He is actively involved in the management and development of several leading firms[44] in this sector. Over the last five years, Estonia has become a global hotspot for crypto companies: as of mid-2021, nearly 55% of all virtual currency service providers in the world were registered in Estonia. Estonia's liberal crypto licensing system enabled such companies – often with non-resident owners and clients – to promote themselves as EU-licensed financial services.

Dmitry is also a representative of three Estonian-based companies engaged in financial service – eWalletex LTD OÜ (fully owned by a Mexican citizen), Kryptoz OÜ (owned by Bulgarian citizen **Ani Valchanova Rezhankova**), IBMCC Limited OÜ (owned by Ukrainian citizen Oleksandr Andreiev, who is a resident of Seychelles and a founder of AC Business Experts DMCC, license corporate service provider[45]).

We have identified BrokerZ, an unregulated FX and CFD broker, operated by Brokerz Ltd from SVG, offshore. The payment processor is ALL MEDIA EOOD, a Bulgarian company founded in 2016 and managed by Ani Valchanova, who also owns Naruda Limited in the UK, which is linked to the scam Way2Finance. Naruda Limited and its network, including Brokerz and associated scam websites, use payment processors like Praxis Cashier, which are known to facilitate scams.[46]

We have identified plenty of regulator warnings for BrokerZ, British FCA, Aussie ASIC, Austrian FMA, Italian CONSOB displayed via Malta MFSA, and also for Naruda Limited from Spain CNMV in 2022.

Summary of Risks Identified in Cases:

The revocation of PayrNet Limited's license in Lithuania due to systematic and multiple violations of local laws, leading to bankruptcy proceedings and potential criminal investigations, highlights the compliance challenges faced by e-payment companies. This revocation impacted associated entities like Payrow and ANNA Money, whose accounts are also available for purchase at the dark market, highlighting the ripple effects of regulatory actions. Similarly, companies like TransferGo and Cryptopay have faced significant fines for AML failures in the UK and Lithuania. Entities like BrokerZ, an unregulated FX and CFD broker, operate from Bulgaria, which has been flagged for facilitating scams and fraudulent activities, further complicating compliance efforts. Numerous e-payment and cryptocurrency companies are based in Estonia, with complex ownership structures and ties to high-risk individuals, presenting significant regulatory challenges. These cases demonstrate how regulatory weaknesses in high-risk jurisdictions contribute to broader compliance issues, emphasizing the need for stronger regulatory oversight and international cooperation to address these systemic vulnerabilities effectively.

We have reached out to Payrow and ANNA with questions about their AML policies, and their awareness of their account sales via dark markets, but no one has responded.

High-risk overview

Compliance failures and regulatory issues are critical concerns in the e-payment sector, especially when operations extend to high-risk jurisdictions. Many e-payment companies face substantial challenges in adhering to AML regulations, leading to frequent license revocations and fines. Jurisdictions with weak regulatory frameworks, such as Malta, Bulgaria, and Estonia, are often taken advantage of because their oversight is not strict enough. This environment creates significant vulnerabilities, allowing illicit activities to flourish. The interconnected nature of these entities means that non-compliance in one jurisdiction can have widespread implications, affecting the entire network. To mitigate these risks, it is essential to strengthen regulatory frameworks, enhance international cooperation, and ensure rigorous enforcement of AML standards across all jurisdictions.

Our research into the exploitation of verified business accounts for money laundering through electronic payment systems has exposed significant vulnerabilities in the current financial and regulatory frameworks. Business accounts, unlike personal accounts, have fewer transaction limits, making them ideal for large-scale illicit activities. Despite strict anti-money laundering measures, these accounts are often sold and used under false identities, enabling undetected money transfers.
We discovered an active market on the dark web where these accounts are bought and sold, often using real identification documents from UK and European citizens. This highlights how criminals exploit gaps in the regulatory systems with sophisticated techniques.

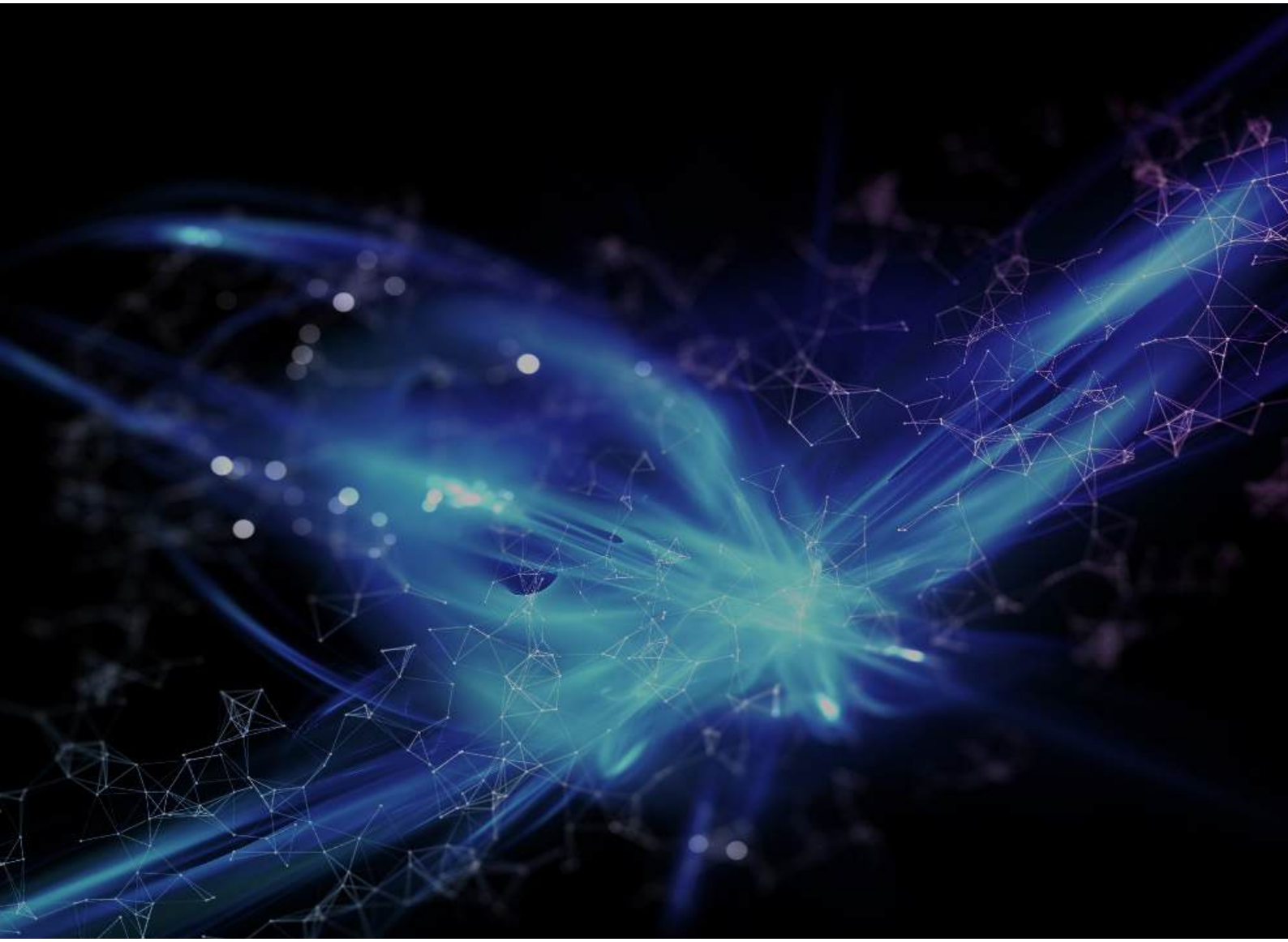
The persistence and growth of these activities, despite existing regulations, reveal critical weaknesses in current AML strategies. This emphasizes the need for stronger regulations, better compliance procedures, and more international cooperation. Enhancing oversight and enforcement, particularly for business accounts, is essential.

CONCLUSION

Our research demonstrates the need for technological advancements to monitor and detect suspicious activities more effectively. Financial institutions must adopt advanced tools, like artificial intelligence and machine learning, to improve their ability to identify and prevent money laundering.

The findings of this report call for a thorough reassessment of current AML frameworks and the implementation of more effective monitoring systems. By addressing these vulnerabilities, regulators and financial institutions can better protect the financial system from illicit funds and ensure greater transparency and security in electronic payment platforms.

In conclusion, our report highlights the urgent need for a comprehensive approach to combat money laundering through verified business accounts. This approach should include stricter regulations, advanced technology, and international collaboration. Only through coordinated efforts can we mitigate these risks and safeguard the integrity of the global financial system.



ENDNOTES

1 https://ti-russia.org/wp-content/uploads/2023/10epaycrypto_.pdf
2 https://www.fca.org.uk/news/press-releases/fca-move-faster-remove-unused-firm-permissions
3 https://www.legislation.gov.uk/uksi/ 2019/1511/regulation/3/made
4 https://www.legislation.gov.uk/uksi/2023/612/part/2/made
5 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/167-defence-against-money-laundering-daml-faq-may-2018/file
6 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/167-defence-against-money-laund ering-daml-faq-may-2018/file
7 https://www.grantthornton.co.uk/insights/fca-guidance-for-payment-and-emoney-firms/
8 https:/psplab.com/license-in-the-uk-and-eea-jurisdiction-attractiveness/
9 https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1056453/Report%20on%20ML%20TF%20risks%20associated%20with%20payment%20institutions.pdf
10 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947842
11 https://www.psr.org.uk/media/ykjf23cs/app-fraud-performance-report-oct-2023_v2.pdf
12 https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/
13 https://www.transparency.org.uk/sites/default/files/pdf/publications/Together%20in%20Electric%20Schemes%20-%20Transparency%20International%20UK.pdf
14 https://find-and-update.company-information.service.gov.uk/company/11040011/persons-with-significant-control
15 Evgeny Zemlyanoy has been working in Gazprom structures since 2007 and has been the Deputy General Director of Economy & Finance at LLC Gazprom Energoholding since 2014. Additionally, according to the Russian corporate registry, Zemlyanoy is the director of LLC GEH Finance, a subsidiary of LLC Gazprom Energoholding. Zemlyanoy holds 25% of shares in LLC PTsFK (Legal Center for Financial Consulting) and 12% of shares in the Russian investment company LLC Mashlizing. Since 2021, he also owns a minority of shares (<0.01%) in two other subsidiaries of LLC Gazprom Energoholding – PJSC TGK-1 and PJSC OGK-2, engaged in the production and sale of electrical and thermal energy.
16 https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=958614&typ=UPLNY
17 https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=76806284&subjektId=958614&spis=1058156
18 Legoshin also denied ever owning Impost LLC, a company based in Russia, although he was a founder until its closure, holding a 66% share.
19 https://medium.com/@thebell.io/forbes-russia-gets-a-new-owner-and-its-journalists-claim-victory-b0fbcd239f8e
20 https://www.yahoo.com/news/forbes-cancels-sale-deal-allegedly-184645154.html
21 Magomed Musaev is also the owner of Forbes Russia since 2018. https://meduza.io/en/news/2018/08/30/old-editors-return-to-forbes-russia-after-its-sale-to-a-new-owner
22 GVA currently manages over $1 billion in assets across three venture funds. The company is jointly based in San Francisco, Moscow, and Almaty.
23 https://sfstandard.com/2022/11/19/russian-oligarchs-big-money-bay-area-investments/
24 https://www.fintechfutures.com/2019/07/paysend-raises-8-5m-for-global-roll-out/
25 https://find-and-update.company-information.service.gov.uk/company/SC562529/filing-history/MzMzNjcz0Tc5MGFkaXF6a2N4/document?format=pdf&download=0
26 Among the shareholders was Lubov Komissarenko, who is reportedly the life partner of Alexander Ponomarenko, the head of Mosvodokanal, a Moscow sewage company. In a joint investigation by Der Spiegel, OCCRP, and Swiss RTS, they were accused of corruption.
27 https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf
28 https://www.transparency.org/en/countries/russia
29 Russia was rated low before 2012 too, but it cannot be compared year by year due to changes in the rating methodology.
30 https://www.cbr.ru/press/PR/?file=10112015_080751ik2015-11-10T08_03_17.htm
31 €282,888
32 As of 2024 The Bank of Russia has revoked the license of Qiwi Bank, known as the operator of Qiwi electronic wallets and the Contact money transfer system, due to violations of federal laws related to anti-money laundering and counter-terrorism financing, as well as conducting risky transactions with the shadow business https://www.cbr.ru/Queries/XsltBlock/File/31947?fileId=26129.
33 Since 2022 OOO PS Processing and OOO Robokassa are fully owned by another Russian company OOO PS Holding. The last one from 2023 is owned by nominees of Abdulkerimov's - Sergey Sigov (90,91%) and Irina Kotova (9.09%).
34 http://www.lb.lt/en/news/licence-of-uab-payrnet-revoked-for-serious-violations-bankruptcy-proceedings-to-be-initiated
35 https://www.railsr.com/payrnet
36 https://news.sky.com/story/british-fintech-railsr-sets-sights-on-growth-after-20m-funding-boost-12993125
37 https://www.bnnbloomberg.ca/payments-firm-that-moved-8-3-billion-last-year-loses-license-1.1936484
38 According to open sources, the UBO of Stylized Enterprises Limited is Dmitry Doykhen and the directors of the company are Russian individuals Nikolay Kutuzov and Valeriy Matveev (who is also a director of Payrow Payment Systems Ltd). https://register.mbr.mt/app/query/get_company_details?auto_load=true&uuid=9f74fef0-dfc3-592c-ab5c-da85edb14608
39 https://anna.money/
40 https://regintel-content.thomsonreuters.com/document/I38A25E80F69111EE9F3C948F717317EB/SPECIAL-REPORT:-Kremlin,-Russian-investors-backed-company-founded-by-KYC-regtech's-leaders-UK-authorised-payment-firms-are-current-entity'scustomers-25-04-2024
41 Mercuryo's Estonian company MoneySwap OÜ had its license revoked by the Estonian Financial Intelligence Unit (FIU) for violations of money laundering regulations in December 2022. https://fiu.ee/tegevusluba-ja-jarelevalve/kehtetuks-tunnistatud-tegevusload
42 https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/
43 https://www.electronicpaymentsinternational.com/news/transferra-sumsub-customer-onboarding/
44 In 2013, Dmitry Lihno founded company, registered in Estonia this time, Private Financial Services OÜ. Currently, the company is in liquidation. The liquidator and the representative of the company is another Ukrainian individual Mykyta Horovoi. We have also identified another representative of the company – Vladislav Drozd, who was also a representative in SkyTech Solutions Group till 2021 mentioned above. According to his Linkedin profile and official Estonian corporate registry, in 2023 he was a UBO of Estonian company AI MInd alongside Dmitry Lihno. He is also a sole shareholder of another Estonian-based company Onhill Capital OÜ engaged in Information technology and computer service activities.
45 https://ac-business.expert/en
46 https://www.eurojust.europa.eu/news/takedown-online-investment-fraud-albania-15-arrests?fbclid=Iw%20AR2zQcDzYadGHeb_WOdrzNRmIvPvRMeu2JKs0AYVwG80wPes15Po55i9-PE

TRANSPARENCY INTERNATIONAL
RUSSIA

WEBSITE

LINKEDIN