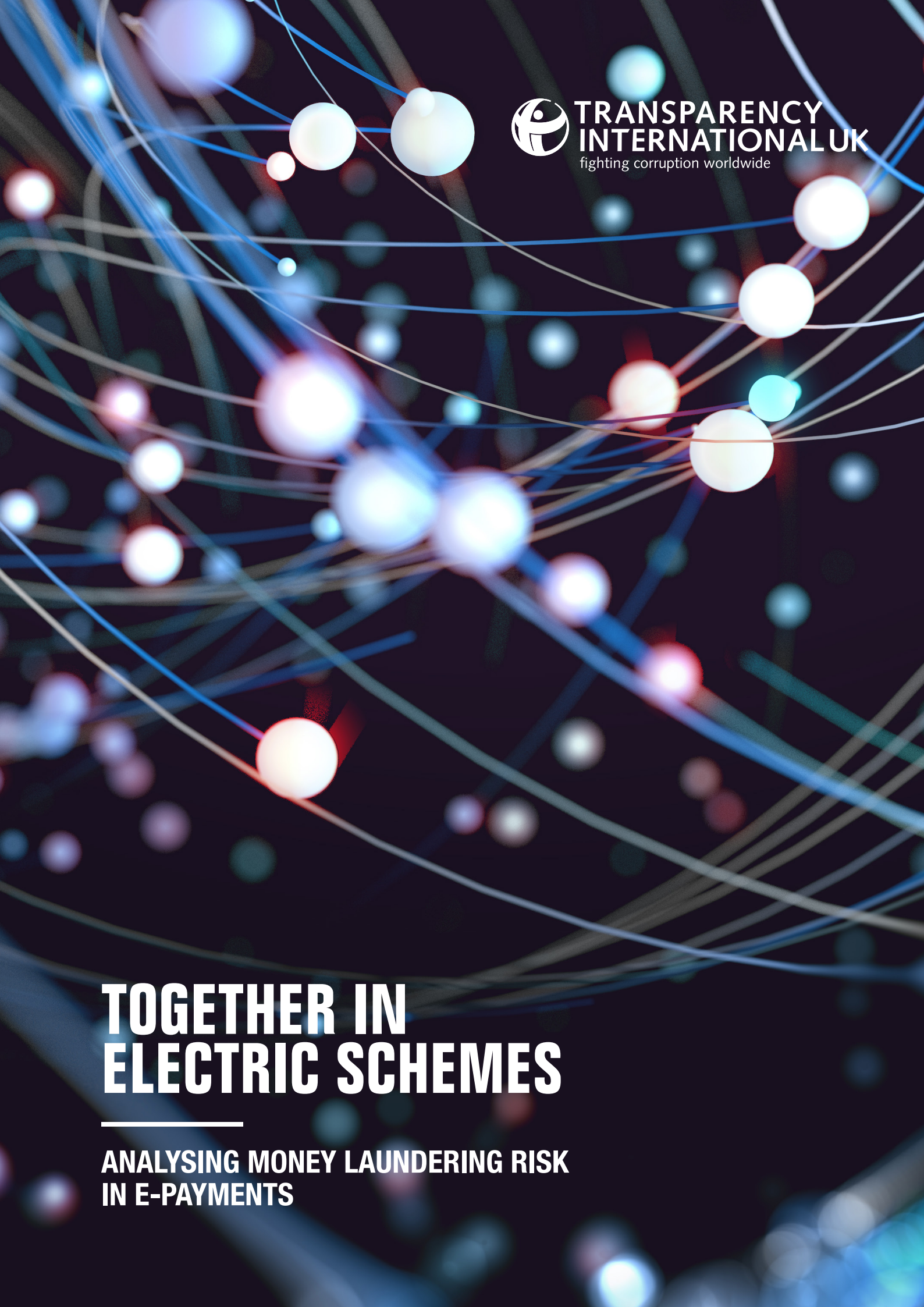


TRANSPARENCY INTERNATIONAL UK
fighting corruption worldwide

TOGETHER IN ELECTRIC SCHEMES

ANALYSING MONEY LAUNDERING RISK IN E-PAYMENTS

Transparency International (TI) is the world's leading non-governmental anti-corruption organisation. With more than 100 chapters worldwide, TI has extensive global expertise and understanding of corruption.

Transparency International UK (TI-UK) is the UK chapter of TI. We raise awareness about corruption; advocate legal and regulatory reform at national and international levels; design practical tools for institutions, individuals and companies wishing to combat corruption; and act as a leading centre of anti-corruption expertise in the UK.

Acknowledgments

We would like to thank Luminate, the Open Society Policy Center and the University of Sussex for their generous support that made the research possible.

We are grateful to Isabella Chase, Paul Heywood, Jane Jee, Nicholas Lord, and Greg Wlodarczyk for providing robust and incisive peer review.

Editor: Steve Goodrich (TI-UK)
Researchers: Ben Cowdock and Georgia Garrod (TI-UK)
Design: Arnold and Pearn

Published December 2021 and updated March 2022

© Cover photo: Carlos Castilla, shutterstock

Printed on 100% recycled paper.

Transparency International UK's registered charity number is 1112842.

CONTENTS

TOGETHER IN ELECTRIC SCHEMES: Analysing money laundering risk in E-Payments

KEY FINDINGS

UK authorised electronic money institutions (EMIs) made more than **£500 billion** worth of transactions in 2020/21

Nearly 1 in 3

Almost one-third **(19,293) reports** to UK law enforcement in 2019/20 relating to **suspected criminal funds** came from the electronic payment sector, which **includes EMIs**

Transparency International UK analysed **261** EMIs authorised by the **Financial Conduct Authority** (FCA) to operate in the UK for **money laundering red flags**

EMI Red Flags

More than **one in three** (100) UK-registered EMIs had money laundering red flags relating to their owners, directors or activities including those:

- named in money laundering investigations and allegations
- holding close links to high-risk firms in Russia and Ukraine
- owned by individuals with question marks over their suitability to run an FCA-authorised firm

Among these owners we found:

- An individual named in the Bank of Cyprus money laundering investigation into the Federal Bank of the Middle East (FBME), an institution that lost its licence after being linked to £760 million (US$1.3 billion) in suspicious payments.
- A formation agent who incorporated hundreds of shell companies reported in suspicious activity disclosures to law enforcement, unveiled as part of the FinCEN Files leak.[1]
- The CEO of a Bitcoin exchange named in the Mueller report as being used by Russian intelligence operatives.

Using open-source analysis we found **EMI licences and accounts for sale** to buyers around the world, including:

- UK EMIs marketing their services specifically to "high-risk" customers and companies with complex ownership structures.
- 38 Russian and Ukrainian language corporate services websites that are selling British EMI accounts alongside secretive offshore companies for clients who want to hide their identities.
- Licenced UK EMIs advertised for sale on LinkedIn and corporate service websites, with prices ranging from £600,000 to £1.5 million.

EXECUTIVE SUMMARY

It has never been easier to manage money and make payments around the world. This is partly due to the rapid growth of the electronic money institutions (EMIs) sector, which offers customers personal and business accounts, global payment services and an alternative to the more traditional banks. These firms are becoming increasingly popular. While most EMIs will be legitimate payment providers, there is a growing body of evidence that suggests they are open to abuse by those seeking to launder corrupt and other illicit funds through the global economy.

In 2020, Wirecard, a major electronic payment processor based in Germany with global operations, collapsed under allegations of mass fraud and money laundering.[2] An investigation by the UK *Financial Times* exposed how the firm had been processing billions of pounds in transactions for high-risk customers.[3] There are now emerging signs that this was not a one-off, and the risk within the sector runs far deeper.

The UK is home to more than 260 EMIs, with a further 77 foreign EMIs offering services here. In July 2021, the UK's biggest EMI, Revolut, was valued at £24 billion, making it worth more than major high street banks like NatWest.[4] The company is only six years old. During this period, not only has it grown dramatically in size, it has also attracted controversy. In 2014, Lithuanian politicians investigated the company over the links between its founder's father and the Russian state-owned natural gas group, Gazprom.[5]

More recently in 2019, a BBC investigation raised concerns over Revolut's anti-money laundering procedures after an employee made a complaint to the Financial Conduct Authority (FCA) claiming the firm's system for identifying illicit funds were "utterly inadequate". While Revolut denies these allegations, the money laundering risks posed by EMIs in the UK are becoming clearer. In 2019/20 almost one-third (19,293) of suspicious activity reports relating to suspected criminal funds came from the electronic payment sector, of which EMIs make up a significant proportion.[6]

This report explores the risks associated with EMIs like these which operate in the UK, and calls for more proactive supervision of their activities than there has been to date. Ignoring this threat could lead to the abuse of EMIs on an industrial-scale like the "Laundromats", as exposed by the Organized Crime and Corruption Reporting Project (OCCRP), that have moved tens of billions of "hot money" out of the former Soviet Union over the past decade.[7]

There are extensive regulations in place stipulating how EMIs must operate, which are overseen by the FCA. These require EMIs to have fit and proper persons in management positions and that they have measures in place to detect and prevent dirty money from moving through the UK economy. However, this research calls into question how rigorously these are being enforced in practice.

Through open-source research, Transparency International UK found that EMIs are already being routinely exposed to illicit funds. We identified 29 (11 per cent) EMIs authorised by the FCA named in adverse media as having ineffective anti-money laundering (AML) controls or processing criminal wealth.

Through analysis of the owners, directors and senior management of EMIs, we identify that many of these individuals have been named in money laundering investigations or held management positions at firms accused of moving dirty money. We found 45 UK EMIs (17 per cent) had owners, directors or senior members of staff named in adverse media. This raises questions as to their suitability as fit and proper persons and reveals that the regulator's checks may fall below the standards they ask of the regulated community they oversee.

Through our review of their relationships with the global financial system, we found 37 EMIs (14 per cent) had owners or directors from the Commonwealth of Independent States (CIS) region, many of whom worked for financial institutions there. Forty-three firms (16 per cent) had links to the Baltic financial sector, either through their owners or through correspondent banking relationships.[8] This region has been an early innovator in the electronic money sector, but became infamous in recent years for its involvement in industrial-scale money laundering, mostly out of the former Soviet Union. Our findings suggest that some of those involved in firms named in money laundering scandals are now migrating to EMIs as an alternative conduit for illicit funds.

EMIs have links to the company formation sector, with some firms owned by former formation agents who incorporated businesses used in money laundering schemes. We found almost 40 Russian and Ukrainian websites offering to form anonymous shell companies and obtain accounts at UK EMIs. Such corporate vehicles provide secrecy over clients' identities and are red flags for money laundering.

We found there is a market for the buying and selling of EMIs, making it more difficult for the FCA to track who controls these firms. There is a cottage industry of professionals who specialise in helping clients obtain EMI licences, which could make it easier for those with pasts to hide and obtain authorisation from the FCA.

As this is a new threat, we do not yet know the likely scale of money laundering through these firms. However, due to the questionable character of those owning certain EMIs and the high-risk markets they are targeting, these firms could soon become a major gateway for illicit funds from around the world, if they are not already.

From reviewing this evidence we recommend three broad areas of action to address this threat before it gets out of control. These seek to:

- **Establish the current threat level posed by EMIs**, with the FCA leading a fresh thematic review of the sector and investigating where firms are named in wrongdoing.
- **Ensure only fit and proper persons manage EMIs**, so they do not become "captured" institutions geared towards laundering money.
- **Encourage a cross-border, multi-sector response to this threat**, taking into account close linkages with foreign banks and company formation agents.

Implementing these recommendations should help head off the emerging money laundering threat posed by EMIs and future-proof the UK's response to illicit finance, enhancing global Britain's reputation as a safe place to do business.

RECOMMENDATIONS

Our research identified nine recommendations in three key areas that should be considered to address the money laundering risks posed by the electronic money sector.

Address the emerging risks posed by the EMI sector

This report highlights critical money laundering risks within the EMI sector that have not yet been addressed in the UK.

RECOMMENDATION 1

The FCA should conduct a new thematic risk review of the sector, with the findings contributing to HM Treasury's national money laundering risk assessment, the National Crime Agency's National Strategic Assessment of Serious and Organised Crime, and the wider law enforcement and anti-money laundering (AML) supervisory response, coordinated by the National Economic Crime Command (NECC).

The UK EMI sector is rapidly evolving with new firms entering the market at a steady rate. This expansion, combined with the risks identified in our research, should be grounds for further investigation by the FCA in coordination with the NECC and HM Treasury.

RECOMMENDATION 2

The FCA should increase monitoring and oversight of EMIs named in money laundering schemes to ascertain whether those firms have appropriate systems and controls in place.

There are a growing number of instances where UK EMIs are identified as being involved in moving illicit funds linked to financial crime. While individually these may be dismissed as one-off events, the growing frequency of these cases suggests a wider trend and that the sector poses an emerging area of risk in need of more hands-on supervision. As a starting point, the adequacy of controls in those firms involved in alleged money laundering should be assessed.

RECOMMENDATION 3

Public and private sector bodies should collaborate to produce an industry alert on the electronic money sector. This would help increase understanding within the broader private sector against the risks posed by illicit finance passing through EMI firms. It would also improve the quality of suspicious activity reports to law enforcement agencies relating to the electronic money sector.

Enhance checks on the owners and directors of EMIs

We have identified a number of individuals involved in the ownership and management of UK EMIs whose past conduct raises questions as to their suitability to run such institutions.

This research has also identified a global market for obtaining UK EMI licences, in part due to the perception that they are subject to fewer regulations and oversight than traditional banks.

RECOMMENDATION 4

The FCA should introduce higher levels of scrutiny to those seeking to control UK EMIs through the fit and proper test. These checks should assess any adverse media and criminal records of all those seeking to control authorised firms.

RECOMMENDATION 5

The FCA should consider close family and business associates in fit and proper testing, to address the risk of criminal networks gaining access to authorised firms by fronting them with those without adverse media.

RECOMMENDATION 6

The FCA's senior managers and certification regime (SMCR) should be extended to all relevant persons working in the EMI industry. This would increase the accountability of senior managers in the sector, lay out minimum behavioural standards and improve the "tone from the top" on AML among these firms.

EMIs are part of the first line of defence against money laundering. They need owners who understand the importance of AML compliance and should not be controlled by those linked to economic crime.

Target high-risk associations between EMIs, company formation agents and overseas banks

This report has identified linkages between UK EMI firms and high-risk firms, including Baltic banks named in major money laundering scandals and company service providers. These companies fall under a number of AML supervisors, covering multiple jurisdictions. These risks require a robust, holistic, cross-border response involving supervisors for the respective sectors.

RECOMMENDATION 7

The FCA should collaborate with national and international money laundering supervisors in addition to the UK Office of Financial Sanctions Implementation (OFSI), to increase understanding of the threats posed by EMIs and coordinate cross-border government, supervisory and law enforcement responses.

As a conduit for international payments, UK EMIs are exposed to global risks. In particular, we identify close links between these firms and financial services provided in Baltic countries and the CIS region, which have been at the centre of industrial money laundering schemes in recent years. These linkages cover financial institutions as well as company formation agents.

RECOMMENDATION 8

The UK government should bring forward Companies House reform as soon as possible to make it harder for criminals to access UK companies.

Current evidence suggests a continuation of past trends, whereby opaque UK shell companies are being abused for financial crimes, albeit this time they are used in combination with EMI accounts and not traditional banks. This is possible because of the current laxness of UK company law, which the government has promised to address. In particular, the lack of checks on those incorporating and controlling UK companies leaves them wide open to abuse by organised criminal gangs and kleptocrats.

RECOMMENDATION 9

The FCA should carry out a targeted audit of the AML compliance of EMI firms marketing their services to high-risk markets.

EMI client markets should be a key consideration when taking a risk-based approach to AML supervision. Given the connections between some EMIs and client markets in the CIS region, which mirror aspects of previous Laundromat schemes, focussing on those marketing services to customers in these jurisdictions should be considered a high priority.

INTRODUCTION

The UK is a global financial hub, with a sizeable financial services industry and banking sector. It is an ideal transit point for moving money and destination for holding assets, with thousands of financial services firms here facilitating more than 40 billion payments a year amounting to around £92 trillion.[9]

Although this connectedness is an asset for global Britain, it is not without its risks. The ease of doing business and scale of transactions leaves the UK exposed to exploitation by criminals seeking to launder corrupt wealth from around the world. While the exact scale of dirty money entering the UK is difficult to quantify, the National Crime Agency (NCA) estimates over £100 billion in illicit funds impacts our economy each year.[10] The UK's financial sector is a key gateway to these financial flows.

Recent years have seen a greater understanding of this issue, with HM Treasury grading the risk of money laundering as high through retail banking, wholesale banking and wealth management services.[11] This assessment rated the UK's electronic money and payment service sector as "medium risk", but noted this was a fast-evolving space, with further monitoring and research needed to gain a better understanding of the threat. This report seeks to help fill this evidential gap by exploring the money laundering risks posed by EMIs in the UK.

As we did not have access to EMI client lists or transaction data, we used open-source material to review the 261 UK firms registered with the FCA as authorised EMIs. This gives us a greater understanding of the nature of money laundering risk in the sector, but not its likely scale.

This analysis explored three key risk areas, which form the main sections of this report:

- Ownership: those controlling these firms and their suitability for the role.
- Associations: the international linkages between UK-registered EMIs and the global financial system, especially where there is a connection to known money laundering issues.
- Markets: their likely customer base to better understand the origin of funds they are handling.

For each EMI authorised in the UK we collected information from Companies House on their owners, shareholders, directors and annual accounts. Using corporate data – including those from leaks like the Panama Papers – as well as information on LinkedIn, we identified further firms these individuals and companies were linked to.

We then searched the names of individuals and firms uncovered through this process, using sources like court documents and news reports, to identify adverse media associated with them.

We have complemented this review with expert interviews with figures from the private sector, public sector, and civil society, and an appraisal of the available literature.

The findings of this analysis are laid out in this report. From our research process we can highlight clear and present risks in this sector that require urgent attention.

Background

EMIs are defined in UK law under the Electronic Money Regulations 2011 as a distinct type of financial firm.[12] To be able to trade legally in the UK, EMIs and anyone seeking to take control of an authorised EMI must seek prior approval from the FCA.

An EMI can offer many of the same services as a high-street bank – from personal and business accounts to international payments – with one key difference: EMIs cannot lend money, meaning they do not offer products like mortgages or business loans.

EMIs attract customers by offering attractive features, including:

- Multi-currency e-wallets, allowing for the storage of different currencies, including cryptocurrencies such as bitcoin, in a single place.[13]
- International payments, often with lower fees than traditional banks.
- Digital banking through online accounts and mobile apps.
- Streamlined online account opening procedures.

The FCA's data on the EMI sector shows that more than £500 billion worth of transactions were made by these firms in 2020/2021.[14] The FCA's data on the EMI sector shows that more than £500 billion worth of transactions were made by these firms in 2020/2021. The UK government estimates that in 2019, British e-money firms held £10 billion worth in customer funds.[15] This figure is likely to have risen since then as the industry has continuedto grow.

These firms play a key role in helping those who may otherwise be unable to access bank accounts to move money across borders, such as migrant workers sending wages back to their families.

EMIs are not able to make international payments, they must have relationships with international "clearing" banks to do this. UK EMIs might not have relationships with UK-based banks and may instead partner with clearing institutions elsewhere in the world. This research has found that it is relatively common for UK EMIs to have correspondent banking relationships with banks outside the UK.

There are currently 261 EMIs authorised by the FCA to operate in the UK. Those seeking an authorisation must submit business plans explaining the services they intend to offer, information on the individuals responsible for these services, as well as details of any person or firm with 10 per cent or more of the capital or voting rights in the EMI.[16] Those controlling[17] these firms are subject to fit and proper tests, which take into account:

- honesty, integrity and reputation
- competence and capability
- financial soundness

The FCA assesses these criteria using sources such as regulatory references, qualification certificates, credit checks, criminal records and directorship checks.

Relevant factors to fit and proper persons may include:

- criminal or civil investigations into a controller
- disciplinary proceedings by a regulator against the controller
- liquidation or insolvency of a business owned or managed by a controller
- the controller's willingness to comply with legal and regulatory standards required of them

Previously, the FCA stated it took into account controllers' relevant family or those with business relationships to the controller.[18] However, this is no longer referred to in the FCA handbook.[19]

The FCA is under a high level of pressure to process requests for authorisation, receiving over 29,000 applications from firms and 55,000 applications from individuals in 2020/21.[20] It currently employs 2,218 people in its supervision and enforcement and market oversight departments who will be tasked with vetting applications as well as overseeing existing firms. With these staffing levels it is unclear how the FCA effectively ensures only appropriate firms and individuals gain authorisation.

The UK's Mutual Evaluation by the Financial Action Task Force (FATF), the global AML standards body, gives further insight into how these checks are conducted, stating that the FCA screens applicants against internal and external databases it holds, but only carries out criminal background checks when concerns are raised relating to a person's fitness and propriety to run a financial institution.[21] Consequently, such checks are only performed in a small proportion of applications.

Once they are authorised, EMIs are expected to report issues such as complaints, instances of fraud, updates on operational risk, and an annual report on the firm's controllers.[22] For applications relating to a change in control of a regulated entity, firms are required to seek approval from the FCA before the change in control takes place. The assessment for this process takes into account the reputation of the proposed controllers and directors of the firm, their financial soundness and whether the risk of financial crime will increase as a result of the acquisition.

EMIs also fall under the UK's Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLRs 2017). These require firms to have AML policies and procedures in place to detect and report the suspected proceeds of crime. This includes requirements to undertake due diligence on their customers,[23] monitoring transactions for suspicious activity, and keeping records of these checks.

The FCA is the AML supervisor for EMIs, meaning it is required to ensure all regulated firms and individuals adhere to the rules.[24] This includes:

- providing advice and guidance on how firms should comply with their legal obligations
- undertaking supervisory activities, such as site visits and audits, to assess whether firms are complying with the rules
- undertaking enforcement action, including imposing civil fines and pursuing criminal convictions where breaches occur

European Economic Area (EEA) EMIs

In addition to UK based EMIs, the FCA has also given temporary authorisation to 77 firms based in the EEA to operate in the UK. These firms are primarily overseen by regulators in their own jurisdictions for money laundering purposes meaning they will be subject to varying levels of oversight depending on the effectiveness of their local AML supervisors. The FCA may take action against these firms if the regulators in their own jurisdictions sanction them.

As displayed in the table below, many of these firms are based in jurisdictions that do not have strong defences against money laundering. A 2021 study of the fintech industry in Lithuania by the local Transparency International chapter noted a lack of capacity of the country's AML supervisors to respond to the rapidly increasing market there.[25]

On 10 June 2021, the FCA issued a ban on Lithuanian firm Finolita UAB from operating in the UK after the Bank of Lithuania rescinded its EMI licence following revelations it was used to funnel €100 million in stolen funds from Wirecard.[26]

In 2021, Malta was placed FATF's "grey list" due to serious weaknesses in its AML defences.[27]

Jurisdiction of EEA EMI with FCA authorisation	Number of EMIs
Lithuania	25
Cyprus	9
Malta	7
Luxembourg	5
Belgium	5
Other	26

Consequently, firms from these jurisdictions offering services in the UK could bring with them additional money laundering risks.

Evidence of abuse

In 2018, the FCA carried out a money laundering risk review of EMIs, which consisted of visiting 13 firms and assessing their AML controls in relation to prepaid cards and digital wallets. It found those reviewed had "reasonably effective anti-money laundering" controls, but did not look at risk relating to the firms' payment services. The findings of this thematic review appear to have informed the FCA's risk-based approach, with the e-money sector not being deemed a priority until recently.[28]

HM Treasury's most recent money laundering supervision report covering 2018/2019 found only 0.6 per cent (97) of the FCA's entire regulated population of 19,660 firms were subject to either a desk-based or onsite review in the one-year reporting period.[29]

Despite the sector being rated as "medium-risk", there is evidence that the sector is increasingly exposed to illicit funds.

Since then, the FCA has reported conducting reviews on 100 payment services firms, which included EMIs. This found several firms were failing to comply with their duties to take appropriate steps to reduce financial crime risk. In July 2020, the FCA announced that the risks to consumers posed by the payment services sector, which included financial crime risks such as money laundering, were a priority area for its 2020/21 business plan.[30] This new focus seems well-justified.

The electronic payments sector is submitting an increasing number of suspicious activity reports (SARs) – disclosures sent to UK law enforcement when firms spot suspected money laundering.[31] In 2017/18, the sector submitted 11,467 reports (2.5 per cent of all SARs that year), which dropped slightly in 2018/19 to 9,517 SARs then increased dramatically to 38,189 reports in 2019/20 (6.6 per cent of all SARs submitted that year).[32, 33, 34] While not all of these will have been submitted by EMIs – with some coming from other payment institutions – this does indicate the sector is increasingly exposed to suspicious funds.

Half the suspicious activity reports submitted by electronic payment firms in 2019/20 (19,293) were "defence against money laundering" (DAML) SARs, where a reporter has a suspicion that property they intend to deal with is in some way criminal.[35] These reports require the UK's financial intelligence unit, housed in the NCA, to analyse the report, allowing them to intervene in the transaction if a criminal investigation relating to the activity is underway or likely to begin as a result of the report. Almost one-third of all DAML SARs submitted by regulated businesses in 2019/20 came from the electronic payment sector.[36]

Our analysis has identified 29 UK EMI firms (11 per cent) with "adverse media" alleging their exposure to dirty money and calling into question their anti-financial crime controls.

This evidence predominantly relates to the proceeds of fraud and cybercrime being processed through UK EMIs. These allegations are based on reports by whistle-blowers and victims of these frauds. Financial crime such as this is typically detected early because the victims are asked to pay funds into accounts at EMI firms, and therefore it is possible to identify the institutions involved.

An investigation by *The Times of Israel* in 2016 named UK EMI MoneyNetInt Ltd as being the subject of a complaint relating to processing payments from a binary options fraud scam.[37] The Polish Financial Supervisor (KNF) issued a warning against MonetNetInt in 2019 for conducting brokering activities without authorisation.[38] MoneyNetInt Ltd states on its website that, "It is the policy of MoneyNetInt, Ltd. to take all reasonable and appropriate steps to prevent persons engaged in money laundering, fraud, or other financial crime."[39] *The Times of Israel* has since stated that there is no evidence that MoneyNetInt is involved in any alleged frauds.

A different fraud scheme investigated by the OCCRP, which impacted over 1,000 people around the world and was orchestrated from Ukraine, involved UK EMI Clear Junction Limited, where victims were asked to make payments to accounts at the firm.[40] In response to the OCCRP, Clear Junction stated that it "carries out all the necessary checks required by UK legislation, as well as according to the best practices of the financial industry and [its] stringent internal procedures."

EMIs have also been reported to have processed payments for organised criminals. In October 2020, Italian media reported that police in the country had identified illicit gambling funds originating from the mafia passing through UK EMIs Skrill and Paysafe.[41] When confronted over these payments, Skrill is reported to have been unable to assist the police with its enquiries. Paysafe said it could not comment on individual cases,[42] that it takes its obligations extremely seriously, and has a comprehensive compliance framework in place to prevent the abusive use of its services.[43]

It is currently unclear to what extent EMIs are being used to channel the proceeds of corruption. Unlike the fraud schemes that have identified UK EMI firms, corruption and associated money laundering can take years to emerge, with law enforcement agencies often reliant on whistle-blowers, leaks and the work of investigative journalists.

FCA interventions into EMIs with weak money laundering controls

The FCA has taken action against a small number of EMIs due to their weak money laundering procedures. In 2019, it halted the operations of a UK EMI, Allied Wallet, after its activities were highlighted in a US investigation into financial crimes committed by the firm and its managers.[44]

In May 2019, the US Federal Trade Commission, an independent agency of the US government, published a press statement on its website stating that a UK EMI, Allied Wallet,

its owner, Ahmad "Andy" Khawaja, and two employees had agreed to settle charges after it was found they had "assisted numerous scams" and knowingly processed fraudulent transactions. Following this judgement, the FCA placed restrictions on Allied Wallet and successfully applied for its liquidation.

While it is positive that the FCA has shown it is willing to take action against firms found to have weak procedures to prevent financial crime, it is unclear how well equipped the FCA is to detect these risks and how reliant the regulator may be on overseas enforcement bodies. Allied Wallet's US branch and Ahmad Khawaja had previously been named in an FBI investigation into laundering illegal gambling payments in 2010. Despite this, Allied Wallet's UK branch was able to successfully seek new authorisation from the FCA four times before it finally had restrictions placed on it.[45]

Recommendations

Our analysis has found a growing number of UK EMIs whose money laundering controls require further scrutiny, due to them being named in adverse media relating to their AML systems and controls. The FCA, law enforcement agencies and private sector firms involved in intelligence sharing should seek to understand money laundering risk in the EMI sector, identify where firms are falling short in their AML obligations and how other parts of the UK economy may be exposed to illicit funds by these firms. This process can be driven in part by focusing on firms this analysis has already identified as being named in adverse media.

RECOMMENDATION 1

The FCA should conduct a new thematic risk report on the sector, with the findings contributing HM Treasury's national money laundering risk assessment, the NCA's National Strategic Assessment of Serious and Organised Crime, and the wider law enforcement and AML supervisory response, coordinated by the NECC.

The UK EMI sector is rapidly evolving with new firms entering the market at a steady rate and related industries like cryptocurrency also in a stage of fast growth. This expansion, combined with the risks our research has identified, should be grounds for further investigation by the FCA in coordination with the NECC and HM Treasury.

RECOMMENDATION 2

The FCA should increase monitoring and oversight of EMIs named in money laundering schemes to ascertain whether those firms have appropriate systems and controls in place.

There are a growing number of instances where UK EMIs are identified as being involved in moving illicit funds linked to high-end financial crime. While individually these may be dismissed as one-off events, the growing frequency of these cases is suggestive of a wider trend and the sector posing an emerging area of risk in need of more hands-on supervision. As a starting point, it seems reasonable to at least assess the adequacy of controls in those firms involved in known money laundering.

RECOMMENDATION 3

Public and private sector bodies should collaborate to produce an industry alert on the electronic money sector. This would increase the understanding of the broader private sector against the risks posed by illicit finance passing through EMI firms. It would also improve the quality of suspicious activity reports to law enforcement agencies relating to the electronic money sector.

Due to the emerging nature of the threat posed by laundering of illicit funds through EMI accounts, the regulated sector must be alerted to the risks posed by the electronic money sector.

OWNERSHIP: WHO CONTROLS UK EMIS?

Understanding who owns UK-registered EMIs is vital to assessing money laundering risk in the sector.

EMIs controlled by individuals from jurisdictions where AML standards are not as high could represent a greater money laundering risk due to their owners not prioritising compliance to detect and report illicit funds. Firms controlled by non-residents also pose a regulatory challenge when seeking to contact or issue sanctions against overseas controllers.

Similarly, firms owned by individuals involved in financial crime or that have previously held roles at institutions with major AML deficiencies are more likely to have weak defences against illicit financial flows or actively facilitate them. Using persons with significant control (PSC) data from Companies House, we identified that those from the former Soviet Union form 21 per cent (45) of natural person PSCs for EMI firms. The Baltic finance sector has been identified as a key conduit for illicit wealth in the past, while Russia and Ukraine are key origin countries for corrupt wealth entering the UK.[46, 47]

Companies House's nationality data is not a perfect measure to understand the geographic spread of owners because PSCs are not obliged to list all their nationalities. For example, one PSC with a common Russian name listed their nationality as Grenadian, a country where it is possible to acquire citizenship in return for investment. Nevertheless, the data available does provide an insight into the geographic connections between EMI management and jurisdictions that are key originators and conduits of hot money out of the former USSR.

Non-resident and corporate owners

Companies House data shows 99 (46 per cent) natural person PSCs of UK EMIs declared they were not UK residents. This may represent a regulatory challenge to the FCA should enforcement action need to be taken against these firms. Eighteen EMIs (7 per cent) claimed they did not have a PSC, which is possible but also questionable.

Our analysis found 99 corporate PSCs[48] controlling UK EMIs, of which 75 were other British firms. The other 24 relevant legal entities came from 16 different jurisdictions.[49] Some EMIs stated their PSCs as companies based in secrecy jurisdictions – such as Cyprus and the Isle of Man – where ownership information is not published. Under UK law there are strict rules over which companies can be listed as owners of other firms on the UK company register. The majority of overseas companies listed as the PSCs of EMIs do not meet the criteria to be listed as an RLE. This is contrary to the intention and letter of the law and obscures ownership of the company, increasing their risk of abuse in financial crimes.

This also poses a challenge to the FCA who will need to continuously monitor ownership of EMIs to ensure only fit and proper persons are involved in their running.

CASE STUDY: Contactpay Solution Ltd

ContactPay Solution Ltd was authorised to operate as an EMI in the UK in June 2021. Its PSC is listed as QIWI PLC, a Cypriot company.[50] QIWI is a Russian payments company that operates around the world. In 2015, an investigation by Radio Free Europe/Radio Liberty alleged that Islamic State militants from the North Caucasus region in Russia were using QIWI to collect funds to finance their activities. In response to this story, QIWI said that it "condemns and does not support terrorist, extremist and other illegal activities" and that it was operating in "strict compliance with applicable legislation including legislation to combat money laundering of criminal funds and terror financing."

"The company is taking all necessary and applicable legal measures to protect its services from penetration by criminal proceeds and also to minimise the risk of the company being involved in the laundering of proceeds from criminal activities and terrorist financing." More recently in December 2020, QIWI announced it was being fined 11 million rubles (£114,000) by the Russian Central bank due to deficient reporting and record-keeping requirements as well as having restrictions placed on its ability to make payments to foreign merchants and money transfers to prepaid cards from corporate accounts.[51] It is unclear whether the FCA took any of these issues into account when authorising QIWI's UK subsidiary, ContactPay.

CASE STUDY: EMIs linked to those from the CIS region

In total, our analysis identified 37 UK EMIs (14 per cent) with owners or directors from the CIS region, predominantly Russia and Ukraine. Many of these individuals held or currently hold links to financial services firms in these countries that have been forced to close, been subject to regulatory or criminal action, or investigated over money laundering concerns. Some examples include:

REMITTANCE360 LTD is a UK EMI that enables customers to send money to more than 50 countries. It lists Maryna Niemkova as one of its PSCs.[52] On her LinkedIn profile, Niemkova listed her experience until July 2018 as "Head of

Remittance System" at TYME – a Ukrainian payments firm. The National Bank of Ukraine terminated TYME's licence in 2018 after Ukrainian security services identified TYME performed money transfers in cooperation with a Russian payment system banned in Ukraine.[53] TYME challenged this decision in November 2018 however the Kyiv administrative court upheld the National Bank of Ukraine's decision.

Maryna Niemkova did not reply to a request for comment on this report.

DECENT FINANCE LIMITED, trading as WLX, is a UK regulated EMI.[54] Decent Finance lists Oleksandr Lutskevych as its PSC, who is also the CEO of bitcoin exchange, CEX.IO.[55, 56] Mr Lutskevych is a Ukrainian National and says he intends to become a UK citizen. Robert Mueller's report into Russian interference in the US 2016 Presidential Elections identified CEX.IO as being used by Russian military agents from the GRU to hold newly minted bitcoin.[57]

Update
Following publication of our report, CEX.IO provided further information in response to our findings. It stated that their due diligence procedures are robust and did not provide any indication that its exchange was being used by GRU agents, and that, as a bitcoin exchange, it would have no way of knowing the ultimate destination of funds or the purpose of transfers.

CEX.IO stated that Decent Finance's EMI license restricts the company's engagement with cryptocurrencies and that the business is currently focussed on serving UK residents. They added that Decent Finance was incorporated after the events in the Mueller Report, in July 2017, and that the company is licenced in the US, Gibraltar, and Canada, and currently has temporary authorisation from the FCA as a crypto-asset business.

Are owners and employees of UK EMIs fit and proper?

While the FCA applies fit and proper tests to all controllers related to EMIs, it is unclear how stringent the regulator is when red flags are identified through this process.

Using investigations by journalists, whistle-blower reports and court documents we identified where owners, directors and senior staff at UK EMIs had previously been linked to financial crimes and irregularities.

This assessment took into account adverse reports which directly named the individual in relation to financial crime and also identified where individuals had worked at another firm involved in such malpractice.

We found 37 EMIs with PSCs or controllers named in adverse reports, constituting 14 per cent of the sector in the UK. Twenty-two EMIs had directors or senior staff named in adverse media (just under 10 per cent of the sector).

CASE STUDY: Euro Exchange Securities UK Ltd

Euro Exchange Securities UK Ltd lists Luis Alberto Gasparini as its PSC. In 2019, the Bank of Spain (Banco de España) fined Gasparini and his company Euro Trading & Financial, S.A. for numerous serious infringements of Spanish banking regulations.[58]

These consisted of:

- Essential irregularities in the accounts of the entity that prevent its financial position from being known.
- Performance of transactions for the sale of foreign currency without the necessary prior authorisation.
- Non-compliance with the obligation to record transactions as stipulated by the Bank of Spain (Banco de España) Circular 6/2001 of 29 October 2001 on owners of a currency-exchange bureau.

As a result Gasparini and Euro Trading & Financial, S.A. were collectively fined €220,800.

Euro Exchange Securities UK Ltd state that the fines related to a different company with a different business model, governed by different laws and regulations. They note that these fines relate to administrative AML and financial infringements rather than predicate financial crime or money laundering offences, and that these infringements were not intentional.

In June 2020, the Dominican Active Multiple Bank (Banco Múltiple Activo Dominicana – BMAD) announced that Gasparini and his son Luis Gasparini Jr, who is a director of Euro Exchange Securities UK Ltd, were to be made vice president and chairman of the board of directors respectively.[59]

The owner of BMAD is reported to be José Antonio Oliveros Febres-Cordero, a Venezuelan banker.[60] Cordero is currently under investigation conducted jointly with the FBI for corruption.[61] It is unclear what, if any relationship, the Gasparinis have to Febres-Cordero.

Euro Exchange Securities UK Ltd state that due to its duty of confidentiality, it cannot give further information on the relationship of the Gasparinis to BMAD.

Euro Exchange Securities UK Ltd's latest set of accounts for the year ended October 2019 states it currently operates in the UK, France, Portugal and Spain with a turnover of £2.5 million.[62]

Fit and proper family members and business associates

While the FCA no longer appears to take into account the conduct of close family members or business associates of those who own EMIs, there is a case for reintroducing this requirement.

EMIs owned by those with close links to individuals involved in serious wrongdoing may be at greater risk of coming into contact with the proceeds of crime.

CASE STUDY: PRIVAT3 Money

PRIVAT3 was incorporated on 28 November 2018 and received its EMI licence from the FCA on 4 March 2020. The company describes itself in job advertisements as "a UK based fintech company specialising in high-net-worth individual payments allowing their customers to be global citizens."[63]

The PSC of PRIVAT3 Money is Réda Bedjaoui, an Algerian-French national with Canadian citizenship and nephew of Algeria's former foreign minister Mohammed Bedjaoui.[64, 65]

Bedjaoui is also the brother of Farid Bedjaoui, nicknamed "Mr 3 per cent", who was the subject of an Interpol Red Notice from 2013 until around 2018 for his alleged role in major corruption cases relating to the Algerian energy sector.[66, 67, 68] Farid Bedjaoui was acquitted in Italy of bribery charges in 2020 but an Algerian investigation into the same case remains ongoing.[69,70] In previous responses to the media, Farid Bedjaoui's lawyers have denied he was involved in any wrongdoing, insisting that, as a 30-something management graduate, he could never have wielded enough influence among Algeria's political, military and business elites to coordinate a US$275-million (£209 million) bribery scheme.

It is unclear if the serious allegations relating to Reda Bedjaoui's brother were taken into account when issuing PRIVAT3's EMI licence.

Reda Bedjaoui has never been charged with, or convicted of, any matter arising from the investigations in Algeria or the now finalized Italian investigations. What is unclear however, is whether the FCA considered his potential exposure to the proceeds of crime when Privat3 was being assessed for authorization.

Links to high-risk institutions

The FCA's fit and proper test also takes into account whether controllers are or were previously involved in businesses that have been investigated, disciplined, censured or suspended by a regulatory body.

Our analysis identified 83 EMIs – almost a third of the sector – where owners, directors or senior members of staff have worked previously for institutions alleged or proven to have AML failings. While not all of those working at EMIs will have been involved in wrongdoing at their former firms, we identified 14 (5 per cent) instances where both owners and directors of EMIs were named in adverse media relating to money laundering failings at firms they previously worked at. Such findings should prompt the FCA to apply even greater scrutiny when assessing whether an EMI's controllers can be considered fit and proper.

CASE STUDY: Guy El Khoury

Guy El Khoury is the owner of the Accomplish Financial group, of which AF Payments Limited has been authorised by the FCA as an EMI since 2018.

Between 2006 and 2012, El Khoury served as CEO of the card services division at the Cypriot bank FBME, which handled transaction processing.[71] On 21 December 2015, the Central Bank of Cyprus revoked the branch licence of FBME bank in Cyprus following the US Financial Crimes Enforcement Network (FinCEN) designating the banking group as "a foreign financial institution of primary money laundering concern".[72]

According to the Times newspaper, leaked audit documents and reports on money laundering issues relating to FBME reveal that its card services division was at the centre of its problems.[73] An investigation into FBME by Kroll on behalf of the central Bank of Cyprus found a number of irregularities including the miscoding of transactions "so that illegal expenditure, high-risk expenditure or other currently unexplained expenditure was recorded as low risk",[74] Mr El Khoury was named as one of a number of senior management alleged to have been aware of the irregularities identified in the the Kroll report.[75]

Guy El Khoury responded stating he only became aware of the wrongdoing at FBME when the suspicion of miscoding was brought to his attention as CEO. He states that his involvement in the activity began when he instructed his staff to terminate a problematic payment gateway.

Further, he states that he is a victim of a misunderstanding in relation to his involvement in the bank's money laundering issues and that it was him that blew the whistle on serious irregularities there before leaving in 2012.

El Khoury also stated in an interview that FBME's card services had been used to assists a sanctioned Iranian bank, Melli, to transact with Iranian customers.[76] El Khoury stated that it was the role of FBME's compliance team to decide on this relationship.

It is not clear if the FCA has read these reports, including The Times article, or taken them into account when authorising AF Payments Limited however they raise serious questions over El Khoury's status as a fit and proper person to run an EMI.

Update

Following the publication of our report, Mr El Khoury made certain complaints, clarifications and other representations which have been updated in our report. Mr El Khoury denies any wrongdoing or complicity in money laundering and we do not allege that he was guilty of money laundering during his time at Card Services. He also denied any awareness of a relationship between Card Services and Melli Bank.

Further, Mr El Khoury states that he underwent stringent vetting procedures to obtain approval from the FSA (as it then was) and then again from the FCA in relation to his UK directorships, and that his full employment history was disclosed as part of the process.

Increasing responsibility and accountability of managers

Currently, the owners and directors of EMIs are not subject to the FCA's senior managers and certification regime (SMCR), which aims to ensure individuals in the financial sector are more accountable for their conduct and competence.

This regime has been extended steadily over an increasingly large part of the financial sector over the past five years, creating a common accountability framework for senior managers and the leadership of firms. It also provides an additional route to enforcement for the FCA when senior managers are found to be in breach of their duties.

Given the risks we have identified in the EMI sector, it would be appropriate to extend the senior managers regime to these firms in order to raise standards of AML practices and create an additional enforcement tool should senior managers fall short in their duties.

Recommendations

EMIs should play a key role in the first line of defence against illicit funds moving through the UK and around the world. Those owned by unsuitable owners are more likely to have weak money laundering controls – or even risk being captured by those seeking to use them to move illicit funds. It is vital that the FCA carries out stringent checks on those seeking to control EMIs to mitigate against this risk.

RECOMMENDATION 4

The FCA should introduce higher levels of scrutiny to those seeking to control UK EMIs through the fit and proper test. These checks should assess any adverse media and criminal records of all those seeking to control authorised firms.

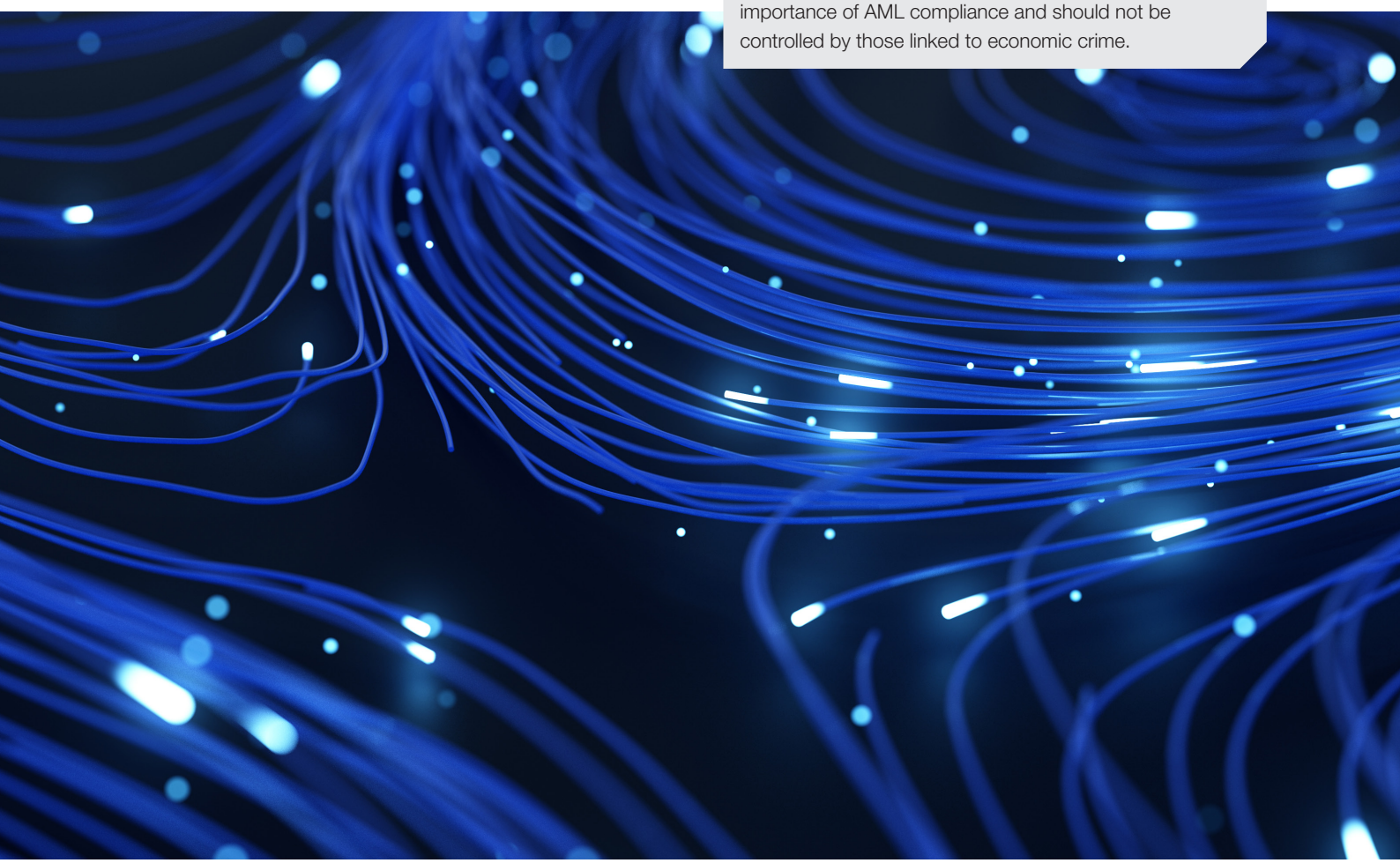
RECOMMENDATION 5

The FCA should take into account close family and business associates in fit and proper testing, to address the risk of criminal networks gaining access to authorised firms by fronting them with those without adverse media.

RECOMMENDATION 6

The FCA's SMCR should be extended to all relevant persons working in the EMI industry. This would increase the accountability of senior managers in the sector, lay out minimum behavioural standards and improve the "tone from the top" on AML among these firms.

EMIs are part of the first line of defence against money laundering. They need owners who understand the importance of AML compliance and should not be controlled by those linked to economic crime.



ASSOCIATIONS: UK EMIS AND THE GLOBAL FINANCIAL SYSTEM

UK EMIs seeking to make international payments for clients need to have relationships with correspondent banks. Our analysis has found a significant number of UK EMIs have close relationships with institutions that have been named in major international money laundering investigations in the past. These international linkages span the globe with those from Venezuelan, Emirati, Russian and Ukrainian financial firms now operating UK EMIs.

If correspondent banks are not doing sufficient checks on institutions they carry out payments for, and UK EMIs do not have sufficient AML controls in place, this creates potential conduits for large amounts of illicit financial flows around the world.

Baltic connections

Our analysis found that 43 (16 per cent) of UK EMIs had relationships with Baltic banks fined for money laundering breaches or named in money laundering investigations, either through owners, directors or employees who had previously worked at financial firms in this region or Baltic banks providing correspondent banking services for UK EMIs.

The Baltic states have emerged as leaders in the fintech industry with innovation drawing many to create businesses there. However, among those seeking to profit from the fintech boom are individuals with histories within some of the region's infamous bad banks, which have been named in money laundering schemes over the past two decades.[77]

This has not happened in isolation. The higher-risk elements of the Baltic banking sector has operated hand in hand with those offering rogue financial services in the UK, which has now been extensively documented in Transparency International research, media investigations and academic literature.

CASE STUDY: Latvian banking connections

This cross-border connection appears to be migrating to the electronic money sector. In 2020, the Latvian Financial Intelligence Unit assessed the country was exposed to increased money laundering risk as a result of flows of money facilitated by Latvian banks on behalf of foreign payment institutions and electronic money firms.[78]

Some Latvian banks now own UK EMIs. Decta Limited, a UK EMI, lists its PSC as Rietumu Holding, the firm behind Rietumu Bank in Latvia.[79] In 2017, Rietumu was fined €80 million by French authorities after it was found to be involved in major tax and money laundering schemes.[80] In response to an investigation by independent global media organisation, openDemocracy, Decta Limited stated it "acts in strict accordance with the requirements of FCA", adding "we regularly pass anti-money-laundering (AML), Anti-Fraud, Know Your Customer and Combating the Financing of Terrorism audits held by Visa, Mastercard and big-four auditors, proving Decta to be complying with all latest AML standards."[81]

In June 2021, Rietumu was fined again for money laundering failings in Latvia, this time in relation to its association with payment service providers, including those based outside of the country.[82] A page on the website of Latvia's central bank (Latvijas Banka), shows Rietumu has correspondent banking relationships with at least six UK EMIs.[83]

It is becoming increasingly clear that British EMIs using Baltic banks for clearing services raises money laundering risk for both the UK and Baltic states. UK EMIs with unsuitable owners or weak AML controls are unlikely to carry out sufficient checks on their clients, while Baltic banks may believe firms regulated by the FCA have higher AML standards than they do in reality. This situation would lead to international payments being made from British EMI accounts using Baltic correspondent banks without sufficient checks being carried out on who was making them. This is similar to the scenario that occurred in the "Laundromats" exposed by the OCCRP, which resulted in billions of pounds in suspicious transactions being sent around the world.

CASE STUDY: Emerald Financial Group (UK) Ltd

Emerald Financial Group (UK) Ltd is an FCA-licenced EMI. The company's website offers a range of services with customers able to "open an account remotely in minutes".[84,85]

According to Emerald's most recently submitted accounts to Companies House, the company has three correspondent bank accounts in Europe and has recently secured an arrangement with a "major UK clearing bank".[86] This will enable Emerald to access almost all global currencies. The company

does not name the correspondent banks located in Europe, nor the major UK clearing bank. Emerald's website shows it is willing to make payments outside the EU of more than €100,000 for "complex" company structures for €120.[87]

Emerald lists three PSCs: Latvians Mark Reckins and Igors Podgorbunskihs as well as Englishman William Matthew Murphy.[88]

According to an investigation by Bne IntelliNews, Reckins previously served as the head of Latvian firm, Financial Group Omega, which formed and administered companies with nominees in a range of secrecy jurisdictions as well as provided bank accounts at Latvian banks.[89] Bne also found that Reckins ran a company called Lotus Corporate Services in the British Virgin Islands (BVI), which has since closed. In 2015, Lotus Corporate Services Ltd was fined US$25,000 (£16,500) for contravention of the BVI's AML and terrorist financing code of practice.[90]

Podgorbunskihs has previously held shares in Latvia's Meridian Trade bank, now named Industra.[91] While his name no longer appears among the bank's shareholders, 14.11 per cent of shares are owned by Natalja Podgorbunskiha, who Russian media report to be his wife.[92]

In 2006, the bank was named Multibanka and was acquired by Russia's SMP bank, which in turn was owned by close associates of Vladimir Putin, Arkady and Boris Rotenburg.[93] Following Russia's invasion of Crimea in 2014, the Rotenburg brothers and their bank were placed on US sanctions lists, and SMP's Latvian branch was sold and renamed Meridian Trade Bank.[94] The bank was fined by Latvia's Financial and Capital Market Commission in 2018 for failures in internal controls, which amounted to breaches of AML rules.[95]

LinkedIn analysis shows three current employees of Emerald who previously worked at the bank now known as Industra, showing further links between Emerald and banks in Latvia named in money laundering investigations.

A Ukrainian company describing itself as an "international law firm" on its Russian/English-language website and which offers company formation services in secrecy jurisdictions, also states that for as little as €200 it will open an account at Emerald.[96]

Neither Emerald Group (UK) Ltd nor its three PSCs replied to a request to comment on this report.

UK EMIs and the company formation agent sector

Our analysis has also found connections between UK EMIs and corporate service providers who have previously formed companies implicated in money laundering. This poses a significant money laundering risk.

Situations where EMIs with correspondent banking relationships work with formation agents who offer to administer opaque companies pose increasingly serious money laundering risks, including the capacity to launder substantial amounts of illicit wealth in multiple currencies with little to no questions asked.

This risk is highlighted by Emerald Financial Group, profiled above, whose third PSC is William Matthew Murphy, who runs a company formation agent called CIE Europe Limited.[97] CIE Europe Limited was fined by HMRC for money laundering failings between 1 August 2019 and 31 January 2020.[98] These breaches of the MLRs 2017 included failures in carrying out risk assessments; not having the correct policies, controls and procedures in place to detect and report suspicious activity; and failures in conducting due diligence.

CIE Europe was also identified as being the formation agent responsible for incorporating a Scottish Limited Partnership that went on to be named in a Ukrainian investigation into organised crime and corruption.[99] No-one returned calls or emails at CIE Europe Ltd when journalists contacted them about these allegations.

Emerald Financial Group and Mr Murphy have not responded to a request to comment on these matters.

CASE STUDY: Dmitrijs Krasko

Dmitrijs Krasko is a Latvian entrepreneur who started his career at ABLV bank, which has now closed after FinCEN designated it a "foreign financial institution of primary money laundering concern".[100] Krasko went on to run a company formation agency that operated in the UK, the Seychelles and Latvia.

Transparency International UK and the International Consortium of Investigative Journalists (ICIJ) have both identified Krasko as having formed and administered companies that went on to be used in money laundering and financial crime.[101,102] This includes 112 companies identified in the FinCEN files database of suspicious transactions. Krasko claimed to have carried out sufficient money laundering checks, stating that there is "no risk to him if the financial statements are false because he insists on an indemnification agreement before signing them".[103] Indemnification agreements do not absolve professionals of any obligation to carry out due diligence checks under the UK's money laundering regulations. In relation to Krasko's above claim, he told us that he was required to enter indemnification agreements in order to provide "trustee services" to companies. He also states that he complied with the Money Laundering Regulations while providing company formation services.

Krasko is also the PSC of a UK EMI, A Plus Payment Solutions Ltd which offers international payments in exchange for 0.2 per cent of the transaction amount.[104]

A Plus Payment Solutions state that neither FinCen nor any other regulator have contacted Dmitrijs Krasko in relation to the companies he formed and administered, whilst his UK formation agency "passed all necessary checks" carried out by HMRC. The company also states that they do not have "a single client who has any relationship to Dmitrijs Krasko's company formation business". A Plus Payments go on to state the FCA were fully aware of Dmitrijs Krasko's previous career as a formation agent. The firm's business plan – approved by the FCA – focuses on attracting clients from the IT industry.

UK EMIs and alternative payment systems

Although many UK EMIs operate through conventional Western financial infrastructures, some have also partnered with alternative payment systems. In 2019, PayXpert, a UK EMI, became the first European acquirer of the Russian Mir card payment system.[105] The Mir card network was set up by the Bank of Russia in 2014 in response to US and EU sanctions over the annexation of Crimea.[106] This saw both MasterCard and Visa cutoff services to several of Russia's main banks. The payment system has grown in popularity in Russia with 73 million cards now issued.[107] Its partnering with international payment service providers makes the country less reliant on traditional financial architecture. This would mitigate the impact of sanctions, enabling those deemed national security risks to continue moving funds around the world.

Recommendations

The money laundering risk posed by EMIs is due in large part to their international associations. EMI accounts can be opened for anonymous shell companies to create opaque money-moving devices. The UK's shell company industry should be targeted to mitigate this risk, which can be achieved through the reform of Companies House in the UK.

Linkages with the Baltic banking sector, which has gained a reputation for facilitating non-resident money laundering, increase the risk that EMIs could be used to move substantial amounts of hot money globally. EMIs are also being used to enable high-risk alternative payment systems to be used in the UK. These issues need cross-government and international cooperation to address.

RECOMMENDATION 7

The FCA should collaborate with national and international money laundering supervisors in addition to the UK Office of Financial Sanctions Implementation, to increase understanding of the threats posed by EMIs and coordinate cross-border supervisory and law enforcement responses.

As a conduit for international payments, UK EMIs are exposed to global risks. In particular, we identify close links between these firms and financial services provided in Baltic countries and the CIS region, which have been at the centre of industrial money laundering schemes in recent years. These linkages cover financial institutions as well as company formation agents.

RECOMMENDATION 8

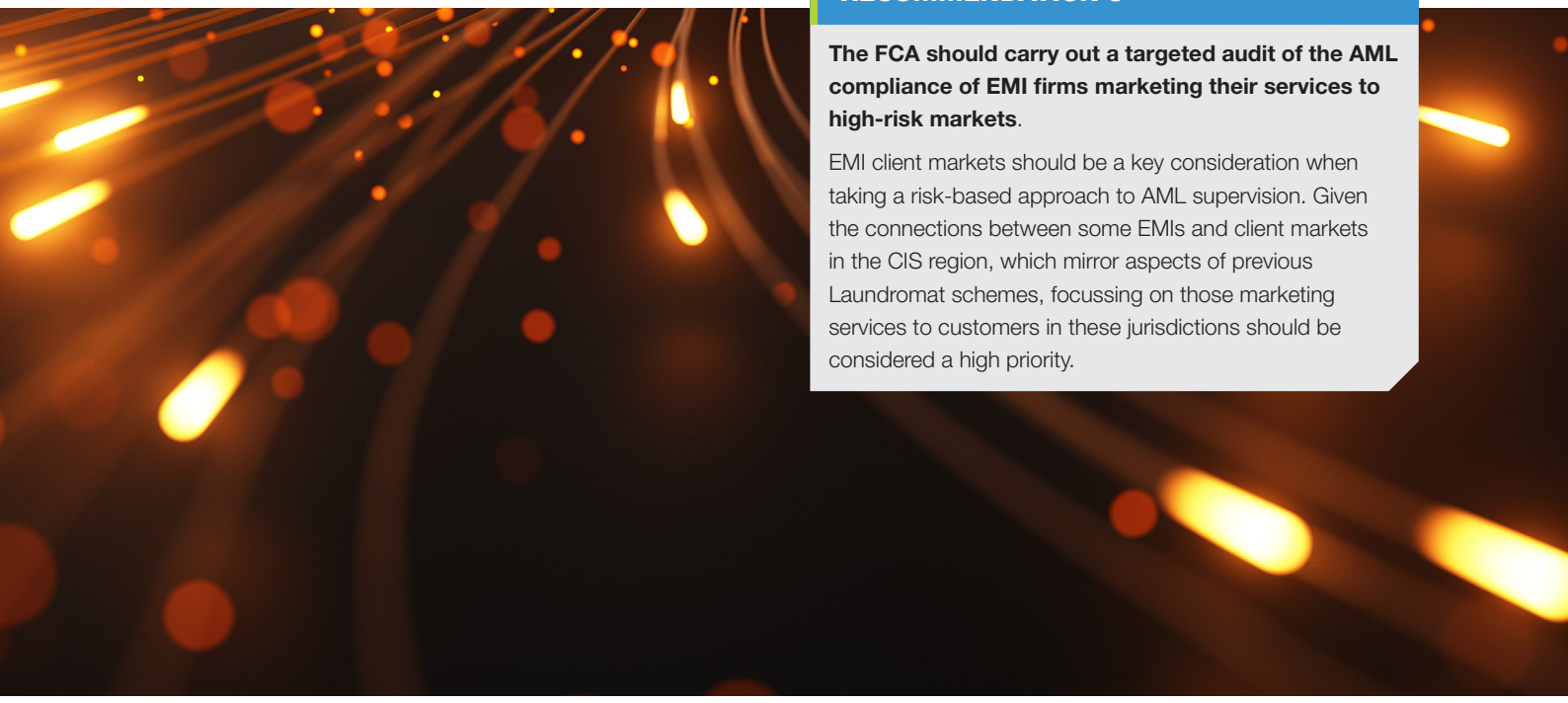
The UK government should bring forward Companies House reforms as soon as possible to make it harder for criminals to access UK companies.

Current evidence suggests a continuation of past trends, whereby opaque UK shell companies are being abused for financial crimes, albeit this time they are used in combination with EMI accounts and not traditional banks. This is possible because the current laxness of UK company law, which the government has promised to address. In particular, the lack of checks on those incorporating and controlling UK companies leaves them wide open to abuse by organised criminal gangs and kleptocrats.

RECOMMENDATION 9

The FCA should carry out a targeted audit of the AML compliance of EMI firms marketing their services to high-risk markets.

EMI client markets should be a key consideration when taking a risk-based approach to AML supervision. Given the connections between some EMIs and client markets in the CIS region, which mirror aspects of previous Laundromat schemes, focussing on those marketing services to customers in these jurisdictions should be considered a high priority.



MARKETS: WHO ARE THEIR TARGET CUSTOMERS?

EMIs have become popular due to their accessibility, ease of use and flexibility in managing the money they offer. They are used by customers from around the world, in part because of how they are advertised to overseas markets.

While the majority of clients they have attracted are customers with legitimate business needs, the way in which EMI services are advertised is likely to attract those seeking to manage criminal finances.

In some areas of the global financial services market, UK EMIs are presented as an alternative for those who are unable to open bank accounts because they are deemed high-risk customers.

IFA consult, a firm headquartered in the UK with a Russian-language website offering company formation and non-resident banking services, refers to "tightening conditions for opening bank accounts" on its marketing page for UK EMIs.[108] Another Russian-language page cited "illogical and sometimes unrealisable requirements from the side of compliance control" and "the requirement for economic presence in the country of registration" as reasons why regular bank accounts were inferior to accounts offered by EMIs.[109]

Using a simple Google search, we were able to find almost 40 Russian- and Ukrainian-language websites offering to set up offshore and UK companies with accounts at UK EMIs for potential clients in former Soviet states.

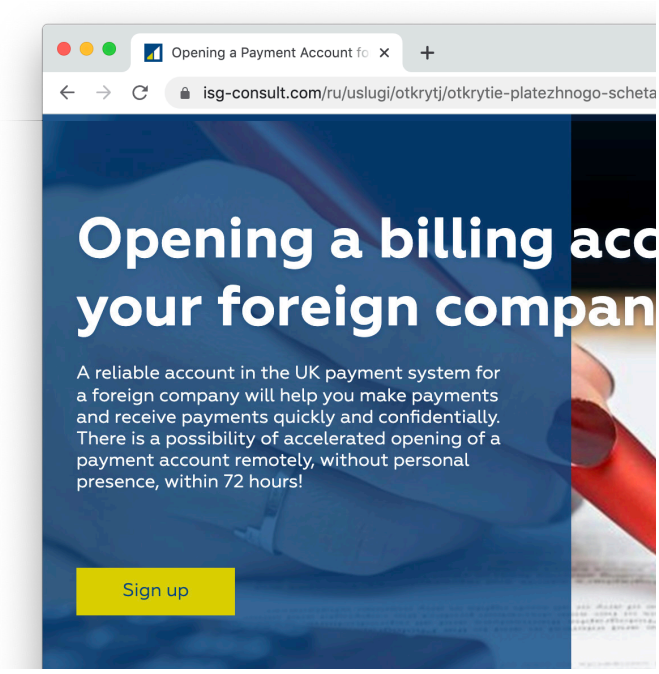


Figure 1: Advert for opening an EMI account for an overseas company.[110]

Fees for opening a corporate account in a UK EMI varied, with one site charging €2,999 for this service at Bilderlings Pay, while another Russian-language website charged €1,000 for opening an account at Emerald, the firm profiled above on page 15.[111, 112]

This combination of being marketed to customers based in high corruption-risk jurisdictions, with fewer due diligence checks than regular banks, along with the possibility of being used by secretive companies based anywhere in the world shows that certain UK EMIs will be exposed to high levels of money laundering risk.

EMI Licences for sale

Not only are EMI accounts being widely sold to those in high-risk jurisdictions but, as highlighted in an investigation by openDemocracy, firms with UK EMI licences are being sold internationally too.[113] Investigators found a company called IQD consulting offering to sell a UK EMI for £1 million.[114] The English-language offer was withdrawn by IGD after openDemocracy got in touch with them.[115]

We found another website claiming to be selling a UK company with an EMI licence for £1.5 million,[116] and other British EMIs being sold openly on LinkedIn for as little as €680,000. These firms were advertised with "clean histories", accounts at major UK banks, as well as those in Latvia and card processing software.

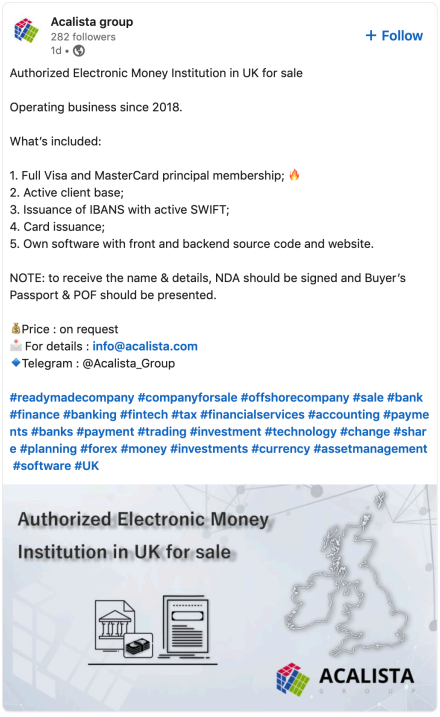


Figure 2: Screengrab fron the Linkedin profile of Acalista group

Another person we identified selling licenced EMIs was Julia Raubishke, currently CEO and owner of corporate service providers Pearly Mount and Round Finance.

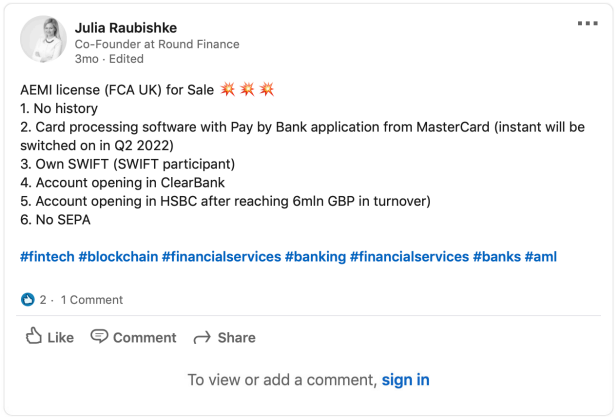


Figure 3: Screengrab from the Linkedin profile of Julia Raubishke

Raubishke had previously worked at Latvian bank BlueOrange between 2012 and 2019. BlueOrange, previously called Baltikums, was fined for money laundering violations by the Latvian Financial regulator in 2018 and has since been reported to have closed 90 per cent of non-resident bank accounts.[117,118] There is no suggestion that Raubishke was involved in wrongdoing at BlueOrange. Between March 2018 and September 2019, she was also a director of a UK EMI, Fincofex, which has since been sold with a view to launching a debit card enabling cryptocurrency to fiat transactions.[119,120]

Savelijs Guzevs, another individual claiming to be an expert in acquiring EMI licences, previously claimed in an interview that UK EMIs are "not subject to banking regulation or related supervision", which is not true.[121] Guzevs currently owns a UK EMI called Azure Psystems Limited. It is unclear if he intends to sell this to a third party.[122]

These examples raise major concerns that UK EMIs could fall into the wrong hands, and makes it more difficult for the FCA to monitor money laundering risk in the sector. As referenced on page 9, the FCA does assess prospective new owners of UK EMIs relating to criteria including the reputation of the new controllers and directors as well as the potential for financial crime risk increasing as a result of the acquisition. This process is likely to encounter similar issues to those we have identified with the FCA's fit and proper testing regime.

CONCLUSION

The EMI sector has seen significant growth over the past five years, with a global market seeking to make international payments with fewer obstacles, and the increasing popularity of cryptocurrency set to continue this trend. This shows the importance of understanding and addressing the money laundering risks brought by the sector.

This report has set out clear and significant emerging money laundering risks with EMIs. Specifically, we identify concerns relating to:

- early signs of their involvement in financial crime
- those who own and control a significant proportion of UK EMIs
- their links to high-risk financial institutions, including problematic parts of the Baltic banking sector
- their marketing alongside corporate secrecy vehicles

The scale of their use in illicit financial flows is currently unknown, with no substantial leaks, regulatory action or court cases as a reliable proxy. However, the evidence we have collected strongly suggests the sector is exposed to large levels of high-risk customers and payments. This increases the likelihood of criminals exploiting EMIs as a gateway into the global financial system.

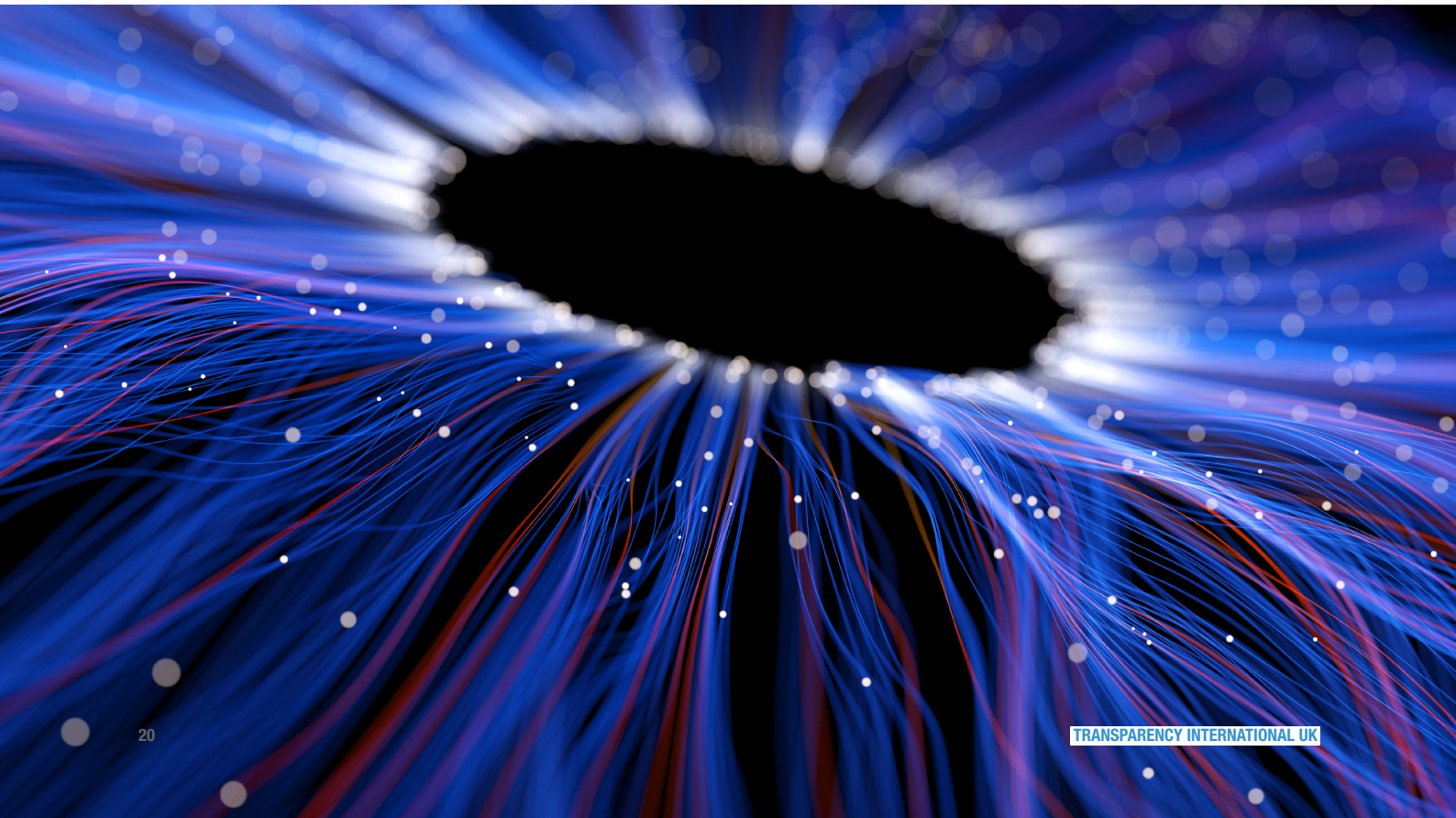
To help address the emerging risks before they spiral out of control, we identify three key areas of action.

Firstly, both the public and private sectors should seek to establish the current threat level posed by EMIs, with the FCA leading a fresh thematic review of the sector and investigating where firms are named in wrongdoing. The public and private sectors should collaborate to create an industry alert identifying key money laundering risks relating to the e-money sector.

Secondly, the FCA should ensure that only fit and proper persons are able to own and operate EMIs. Those who have played leading roles at firms involved in high-end money laundering and financial crime should not be able to operate financial institutions in the UK. This principle should extend to the close relatives and business associates of EMI owners.

And thirdly, to address the international money laundering risk posed by UK EMIs, the correspondent banking system and company services providers, the FCA and the NCA should establish a cross-border, multi-sector response to this threat.

By acting early, the threat posed by this sector can be addressed, protecting victims of corruption and financial crime and safeguarding the UK's role as a safe and clean global financial hub.



ENDNOTES

1 www.icij.org/investigations/fincen-files/ [accessed: 20 October 2021].
2 www.moneylaunderingnews.com/2020/07/wirecard-a-scandal/ [accessed: 21 July 2021].
3 www.ft.com/content/af783224-2348-4ed7-87ec-5bb9ada06eea [accessed: 21 July 2021].
4 www.bbc.co.uk/news/business-57854969 [accessed: 21 July 2021].
5 Ibid.
6 UK Financial Intelligence Unit, *Suspicious Activity Reports Annual Report 2020*, (London: NCA,2020).
7 www.occrp.org/en/laundromats/ [accessed: 21 July 2021].
8 www.riskscreen.com/kyc360/news/imf-asked-to-evaluate-nordic-and-baltic-money-laundering-prevention/ [accessed: 21 July 2021].
9 www.ukfinance.org.uk/sites/default/files/uploads/Summary-UK-Payment-Markets-2021-Final.pdf [accessed: 13 October 2021].
10 www.nationalcrimeagency.gov.uk/news/national-economic-crime-centre-leads-push-to-identify-money-laundering-activity [accessed: 21 July 2021].
11 HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, (London: Home Office, 2020).
12 Electronic Money Regulations 2011 https://www.legislation.gov.uk/uksi/2011/99/regulation/1/made.
13 Note cryptocurrencies are not covered by the rules governing EMIs, but any firm trading in these assets here must comply with the UK's money laundering regulations www.fca.org.uk/consumers/cryptoassets [accessed: 1 November 2021].
14 FCA response to Transparency International UK Freedom of Information Act request [received: 18 November 2021]
15 HM Treasury, *Payments Landscape Review: Call for Evidence*, (London: UK gov, 2020).
16 Financial Conduct Authority, *Payment Services and Electronic Money – Our Approach*, 2017 (London: FCA, 2017).
17 A controller is defined as any person holding 10 per cent or more of the shares in capital or voting power of the applicant business (or 10 per cent or more of shares in capital or voting power of a parent of the applicant) or is otherwise able to exercise significant influence over the management of the applicant business through shareholding or voting rights
18 Financial Conduct Authority, *The FCA's role under the Electronic Money Regulations 2011 – Our approach* (London: FCA, 2013).
19 Financial Conduct Authority, *Fit and Proper test for Employees and Senior Personnel sourcebook*, (October 2021) https://www.handbook.fca.org.uk/handbook/FIT.pdf
20 FCA, *Annual Report and Accounts 2020/21*, (London: FCA, 2021).
21 Financial Action Task Force, *Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report*, 2018, (London: FATF, 2018).
22 www.fca.org.uk/firms/reporting-requirements-payment-institutions [accessed: 21 July 2021].
23 This includes identifying and verifying customers obtaining beneficial ownership information, and taking enhanced due diligence measures for higher-risk customers
24 www.legislation.gov.uk/uksi/2017/692/regulation/46/made [accessed: 1 November 2021].
25 www.transparency.lt/en/during-the-pandemic-the-scale-of-fraud-using-fintech-companies-has-likely-increased/ [accessed: 21 July 2021].
26 www.fca.org.uk/publication/supervisory-notices/first-supervisory-notice-uab-finolita-unio-2021.pdf [accessed: 21 July 2021].
27 www.reuters.com/business/global-dirty-money-watchdog-adds-malta-grey-list-keeps-pakistan-2021-06-25/ [accessed: 21 July 2021].
28 Financial Conduct Authority, *Money Laundering and Terrorist Financing Risks in the E-Money Sector*, October 2018, (London: FCA,2018).
29 HM Treasury, *Anti-money laundering and counter-terrorist financing: Supervision report 2018-19*, August 2020, (London: HM Treasury,2020).
30 https://www.fca.org.uk/publication/correspondence/payment-services-firms-e-money-issuers-portfolio-letter.pdf [accessed: 1 November 2021].
31 SARs are sent to the UK's Financial Intelligence Unit (FIU), which is housed in the NCA
32 UK Financial Intelligence Unit, *Suspicious Activity Reports Annual Report 2018*, (London: NCA, 2018).
33 UK Financial Intelligence Unit, *Suspicious Activity Reports Annual Report 2019* (London: NCA, 2019).
34 *Suspicious Activity Reports*, n6.
35 Ibid.
36 Ibid.
37 www.timesofisrael.com/follow-the-money-how-one-defrauded-binary-options-investor-got-his-cash-back/ [accessed: 21 July 2021].
38 www.iosco.org/investor_protection/investor_alerts/pdf/uploads/93165F9D-B083-FEC0-B007728F9EAD4C1D/ALERT_MoneyNetInt.pdf [accessed: 21 July 2021].
39 https://cdn2.hubspot.net/hubfs/2625488/MoneynetInternational_Nov2016/Docs/MNI%20-%20AML%20Policy.pdf?t=1532866971453 [accessed: 21 July 2021].
40 www.occrp.org/en/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center [accessed: 21 July 2021].
41 https://irpimedia.irpi.eu/en-paysafe-e-wallets-mafia-transactions/ [accessed: 21 July 2021].
42 Ibid.
43 Ibid.
44 www.fca.org.uk/news/statements/allied-wallet-limited [accessed: 21 July 2021].
45 https://vixio.com/insight/paymentscompliance/a-step-change-in-supervision-the-fcas-crackdown-on-payments-comes-after-years-of-little-scrutiny/ [accessed: 21 July 2021].
46 G. Stack, "Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space", *Journal of Money Laundering Control*, 5 January 2015.
47 Transparency International UK, *At Your Service: Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations* (London: TI-UK,2019).
48 Known in law as relevant legal entities (RLEs), which are permitted so long as they provide their own PSC register or are subject to equivalent beneficial ownership requirements in another jurisdiction.
49 Note some companies were registered as RLEs for multiple EMIs.
50 https://find-and-update.company-information.service.gov.uk/company/12149419/persons-with-significant-control [accessed: 17 September 2021].
51 https://investor.qiwi.com/static-files/725e0c58-f64a-4986-8853-f65c21d07b0e [accessed: 17 September 2021].
52 https://find-and-update.company-information.service.gov.uk/company/12181797/persons-with-significant-control [accessed: 21 July 2021].
53 https://ukranews.com/en/news/569032-nbu-terminates-registration-of-tyme-international-payment-system [accessed: 21 July 2021].
54 https://wlxwallet.com/contact [accessed: 21 July 2021].
55 https://find-and-update.company-information.service.gov.uk/company/10871225/persons-with-significant-control [accessed: 21 July 2021].
56 https://blockchain.news/interview/exclusive-cex-io-the-holistic-bitcoin-exchange-taking-the-us-regulatory-road-less-travelled [accessed: 21 July 2021].
57 US Department of Justice, *Report on the investigation into Russian interference in the 2016 presidential election*, 2019. (Washington D.C.: US government, 2019).
58 www.bde.es/bde/en/areas/supervision/sancion/sanciones-impues/index201902.html [accessed: 21 July 2021].
59 https://acento.com.do/economia/banco-activo-anuncia-cambios-en-su-consejo-de-administracion-8827136.html [accessed: 21 July 2021].
60 Dominican Active Multiple Bank, Annual Report 2019.
61 https://porlanoticia.com/index.php/2019/10/08/autoridades-de-ee-uu-investigan-a-banquero-jose-antonio-oliveros-febres-cordero-de-banco-activo/ [accessed: 21 July 2021].
62 https://find-and-update.company-information.service.gov.uk/company/06409565/filing-history/Mzl4MzcyMTE1OGFkaXF6a2N4/document?format=pdf&download=0 [accessed: 21 July 2021].
63 www.privat3money.com/ [accessed: 21 July 2021].
64 https://find-and-update.company-information.service.gov.uk/company/11700691/persons-with-significant-control [accessed: 21 July 2021].
65 www.icij.org/investigations/panama-papers/20160725-natural-resource-africa-offshore/ [accessed: 2 November 2021].
66 https://fcpablog.com/2016/07/27/report-panama-papers-show-role-of-shell-companies-in-saipem/ [accessed 24 November 2021]
67 www.nytimes.com/2016/07/25/world/americas/panama-papers-reveal-wide-use-of-shell-companies-by-african-officials.html [accessed: 21 July 2021].
68 www.icij.org/investigations/panama-papers/oil-giant-eni-to-pay-millions-over-sham-contracts-in-panama-papers-bribery-case/ [accessed: 21 July 2021].
69 www.sec.gov/enforce/34-88679-s [accessed: 21 July 2021].
70 www.theafricareport.com/32969/two-corruption-cases-rattle-sonatrach-in-algeria-and-lebanon/ [accessed: 21 July 2021].
71 www.pressreader.com/cyprus/financial-mirror-cyprus/20091202/282385510609741 [accessed: 21 July 2021].
72 https://www.fincen.gov/sites/default/files/special_measure/FBME_FR_20160325.pdf [accessed: 21 July 2021].
73 www.thetimes.co.uk/article/mastercard-allegedly-linked-to-phantom-transactions-n8p0kkpmn [accessed: 21 July 2021].
74 Kroll, *FBME Bank Review 2015*, para 3.1 p.12.
75 Kroll, *FBME Bank Review 2015*, para 3.3.1.4 p.20
76 Kroll, *FBME Bank Review 2015*, para 3.6.2 p.30
77 www.riskscreen.com/kyc360/news/imf-asked-to-evaluate-nordic-and-baltic-money-laundering-prevention/ [accessed: 21 July 2021].
78 Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017–2019 (2020).
79 https://find-and-update.company-information.service.gov.uk/company/09926210/persons-with-significant-control [accessed: 2 November 2021].
80 www.occrp.org/en/daily/6697-latvian-bank-fined-80-million-for-money-laundering-will-appeal [accessed: 21 July 2021].
81 www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/ [accessed: 2 November 2021].
82 www.fktk.lv/en/news/press-releases/fcmc-imposes-a-fine-and-legal-obligations-on-as-rietumu-banka/ [accessed: 2 November 2021].
83 www.bank.lv/en/legal/payment-and-settlement-systems/legal/target2/559-payment-and-settlement-systems/2714-electronic-clearing-system-eks [accessed: 21 July 2021].
84 www.emerald-financialgroup.com/ [accessed: 21 July 2021].
85 Ibid.
86 https://find-and-update.company-information.service.gov.uk/company/11557885/filing-history/Mzl3NjQxMjkwMGFkaXF6a2N4/document?format=pdf&download=0 [accessed: 21 July 2021].
87 https://emerald24.co.uk/wp-content/uploads/2021/05/Business-Fees-1.pdf [accessed: 21 July 2021].
88 https://find-and-update.company-information.service.gov.uk/company/11557885/persons-with-significant-control [accessed: 21 July 2021].
89 www.intellinews.com/career-of-shell-company-creator-points-to-banks-as-culprits-500017931/?archive=bne [accessed: 21 July 2021].
90 Ibid.
91 www.delfi.lv/bizness/bankas_un_finanses/rietumu-sankciju-skarta-latvijas-banka-pern-nopelnijusi-217-000-eiro.d?id=45641540 [accessed: 21 July 2021].
92 https://lv.sputniknews.ru/economy/20191126/12814138/Obezopasit-tranzit-zachem-Meridian-Trade-Bank-portovym-oligarkham.html [accessed: 21 July 2021].
93 https://uawire.org/joint-media-investigation-reveals-that-russian-oligarch-owns-villas-on-the-french-riviera [accessed: 21 July 2021].
94 https://www.globenewswire.com/news-release/2014/06/17/644578/0/en/The-new-name-of-AS-SMP-Bank-is-AS-Meridian-Trade-Bank.html [accessed: 21 July 2021].
95 www.fktk.lv/en/news/press-releases/fcmc-imposes-a-fine-and-legal-obligations-on-as-meridian-trade-bank/ [accessed: 21 July 2021].
96 www.maira-consult.com/services/accounts/emerald24 [accessed: 21 July 2021].
97 https://find-and-update.company-information.service.gov.uk/company/08128457/persons-with-significant-control [accessed: 21 July 2021].
98 www.gov.uk/government/publications/businesses-not-complying-with-money-laundering-regulations-in-2018-to-2019/list-of-businesses-for-tax-year-2019-to-2020-that-have-not-complied-with-the-2017-money-laundering-regulations--2 [accessed: 21 July 2021].
99 www.heraldscotland.com/news/14641519.fuerteventura-inter-scots-firm-centre-organised-crime-probe-weapons-deal/ [accessed: 21 July 2021].
100 www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and [accessed: 2 November 2021].
101 *At Your Service*, n42.
102 www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/ [accessed: 21 July 2021].
103 Ibid.
104 https://static1.squarespace.com/static/5cc1a45b8dfc8c78718d04a2/t/5d8cd8d49a9ef27a6b0f3a

bd/1569511636838/Pricing.pdf [accessed: 15 October 2021].

105 https://blog.payxpert.com/the-first-european-acquirer-of-the-mir-card-scheme-is-unveiled-at-the-russian-british-business-forum [accessed: 21 July 2021].

106 www.reuters.com/article/us-russia-cards-idUSKCN1RV0KZ [accessed: 21 July 2021].

107 https://apexx.global/blog/how-russias-mir-marries-state-goals-with-payments-disruption [accessed: 21 July 2021].

108 https://ifa-consulting.com/services/bank-accounts/platezhnie-sistemy/ [accessed: 21 July 2021].

109 www.isg-consult.com/ru/uslugi/otkrytj/otkrytie-platezhnogo-scheta-dlya-vashej-inostrannoj-kompanii [accessed: 21 July 2021].

110 Ibid.

111 https://internationalwealth.info/best-offshore-services/corporate-account-british-payment-bilder-system-lings-pay/ [accessed: 21 July 2021].

112 https://ybcase.com/ps-reviews/emerald [accessed: 21 July 2021].

113 www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/ [accessed: 21 July 2021].

114 Ibid.

115 Ibid.

116 www.mergerscorp.com/property/electronic-money-institution-emi-license-for-sale-in-uk/ [accessed: 21 July 2021].

117 www.reuters.com/article/latvia-moneylaundering-idUSL8N1YQ51H [accessed: 21 July 2021].

118 www.lrt.lt/en/news-in-english/19/1236645/fincen-leaks-in-baltics-latvia-exposed-as-high-risk-jurisdiction [accessed: 21 July 2021].

119 https://find-and-update.company-information.service.gov.uk/company/11246175/filing-history [accessed: 21 October 2021].

120 www.altcoinbuzz.io/cryptocurrency-news/product-release/swipe-acquires-fincofex-to-launch-swipex/ [accessed: 21 October 2021].

121 https://mundooffshore.net/licencia-de-entidad-de-dinero-electronico/ [accessed: 21 July 2021].

122 https://find-and-update.company-information.service.gov.uk/company/12108869/persons-with-significant-control [accessed: 21 July 2021].

Transparency International
10 Queen Street Place,
London,
EC4R 1BE

transparency.org.uk
twitter.com/@TransparencyUK

Transparency International UK

Registered charity number 1112842

Company number 2903386