Government of JERSEY

Money Laundering Typologies

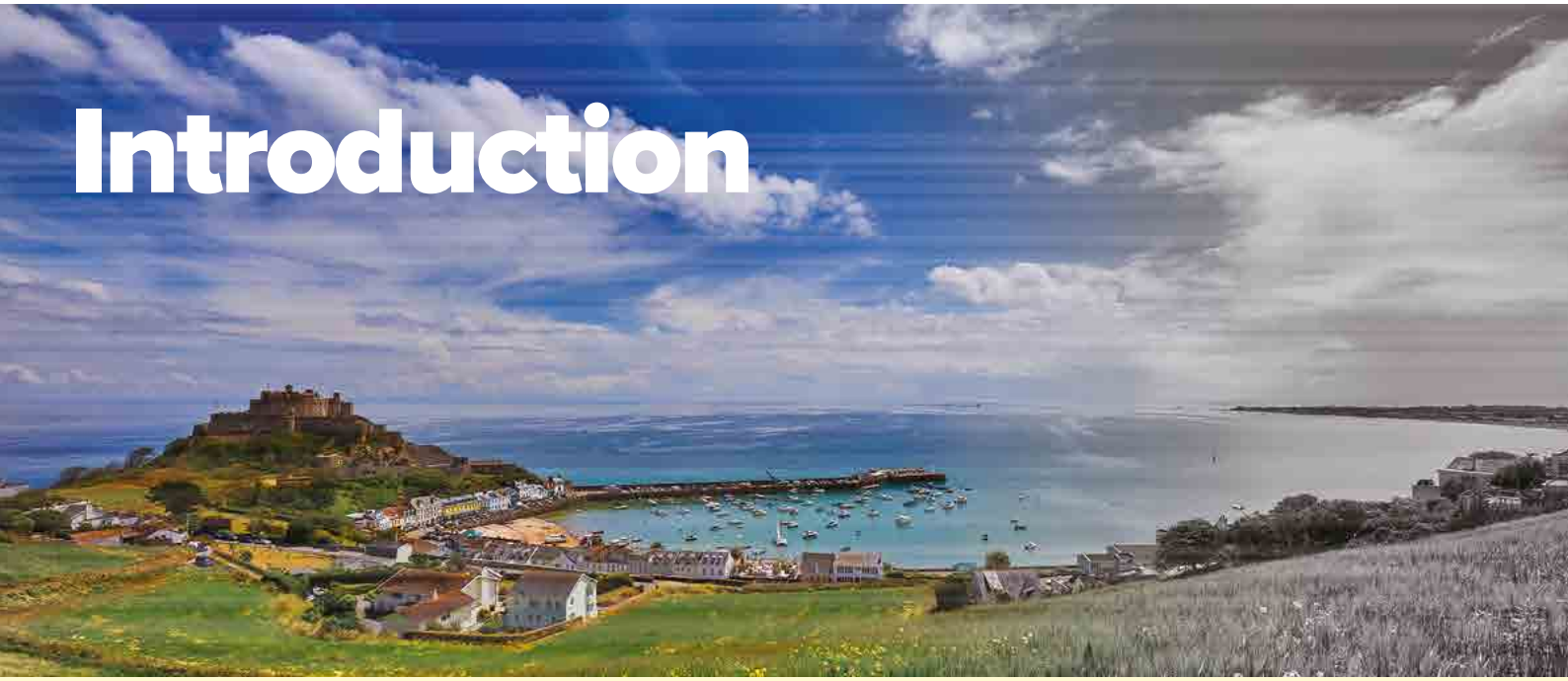
Produced by Baker Regulatory Services Limited

- Issued by the Joint Financial Crimes Unit & the Financial Intelligence Unit - January 2023

> “Targeting the money laundering aspect of criminal activity and depriving the criminals of their ill-gotten gains, hits them where they are vulnerable. Without access to usable profits, the criminal activity will not continue.”

Detective Inspector Louise Clayson
FIU Jersey

Contents



Introduction

Financial crime is constantly evolving and becoming more sophisticated and complex, meaning that new threats are regularly emerging for Jersey. As an International Finance Centre, Jersey is inevitably exposed to money laundering threats. We have a social and economic duty to detect and prevent these threats. The money laundering typologies contained within this document provide key red flag indicators to be aware of when assessing if suspicious activity could indicate money laundering and provides links to further helpful reading on the type of money laundering highlighted by the typology.

The typologies take into account the money laundering risks identified in Jersey's National Risk Assessments and draws upon the financial crime intelligence held by the Jersey Financial Intelligence Unit and also the experience of law enforcement officers, regulators, the finance industry, litigators and insolvency practitioners.

> "We have a social and economic duty to detect and prevent these threats."

In compiling the typologies, emphasis has been placed on including the most prevalent types of money laundering that our finance industry may be exposed to, but also emerging risks seen globally and identified by our international partners. Where cases have been successfully prosecuted the link to the full judgment is provided to allow readers the opportunity to gain a deeper understanding of how the money laundering occurred.

The typologies are divided into sector specific examples, under the headings of Banking, Funds Services Business, Trust and Company Service Providers, Investment Business, Insurance, Money Services Business, Estate Agents, Dealers in High Value Good and Legal Professionals.

The document also acts as a self-learning tool with links to other helpful credible material available online, culminating in a knowledge check enabling readers to verify their understanding of the red flags associated with sector specific money laundering risks.

This document will be updated annually and reissued. If you consider that an emerging typology should be included in the next update please email the details to the Jersey Financial Intelligence Unit at fiu.admin@jersey.jersey.police.je

As you will see from the judgments identified in this document, Jersey has in the past led in the fight against money laundering and understanding the modus operandi that criminals use to launder their ill-gotten gains. By studying this typology document you will help us in the continuing fight against financial crime and removing the profits out of the hands of criminals, seizing such assets and using confiscated assets to reduce the impact of financial crime upon society.

Thank you for taking the time to read our document.

Detective Inspector Louise Clayson

Head of the Jersey Financial Intelligence Unit

Produced by Baker Regulatory Services Limited.

Particularly relevant to the following sectors – Banking/TCSP/Estate Agents/Lawyers and Accountants/Auditors.

In 2020 one of the most frequent offences reported to the Jersey Financial Intelligence Unit via suspicious activity reports continued to be suspected tax fraud with 24.5% of all SARs submitted on the basis of the submitting institution suspecting fiscal/revenue fraud. In 2021 this figure was 21.1%. Jersey's National Risk Assessment concluded that Tax Evasion posed one of the most significant money laundering risks to the Island https://jersey.police.uk/media/622818/JFIU-Statistical-Report-2020.pdf

Tax Evasion Typologies

Tax evasion is an illegal activity often involving the misrepresentation of the tax payers affairs in which a person or entity deliberately avoids paying a true tax liability.

TYPOLOGY 1

Local business woman convicted of drug trafficking and tax evasion.

As part of a wider operation Joanne Jones' car-wash business premises in Jersey were searched and slightly under 500g of cannabis resin was discovered. Jones pled guilty to possession with intent to supply on the basis that she had been minding the cannabis temporarily for another whom she was not prepared to name, without financial reward.

Investigations of Jones' bank accounts revealed substantial funds which she insisted came from several legitimate sources. She was tried on counts of laundering the proceeds of drug trafficking and was acquitted after a two week trial in 2018 having successfully argued that the money that had flowed through her bank account was not attributable to drug trafficking but originated from income derived from her legitimate businesses - albeit undeclared to the Comptroller of Income Tax. She pled guilty and was subsequently sentenced for failing to declare the legitimate income to the Comptroller over a six year period, and to three counts of money laundering namely, possessing, controlling, converting or transferring criminal property relating to unpaid tax.

The Income Tax offences took place over 6 years and were admitted under declaration of what the Crown accepted were legitimate earnings amounting to £263,558.55, on which there was unpaid income tax of £59,242.27 together with a 10% surcharge and payments due under the long term care scheme, which gave rise to a total sum due to the Comptroller of £65,825.99.

The money laundering offences related to the concealment of the proceeds of the crime of income tax evasion, namely the £65,825.99 that she kept for herself instead of paying it to the tax authorities as required by law. Jones had effectively filed false returns with the Income Tax Department.

The court concluded that the offences of drug trafficking and the tax evasion should be marked by a sentence of imprisonment, not only to punish the defendant but also to send a message to others considering embarking upon similar fraudulent activity.

Jones was sentenced to a total of 20 months imprisonment and a total fine of £75,000. In addition, the sum of £65,852.99 was paid to the Comptroller of Income Tax from her restrained assets.

Red flags

- Significant volumes of cash intermingled with the revenue from legitimate business income.
- Criminal activity included a combination of drug trafficking and tax fraud.

Learning points

1. The case highlights the importance of transaction monitoring, particularly cash deposits and comparing the expected volume of activity on the account as described at the onboarding stage.
2. Establishing the details of the beneficial owner and controller of the several legal entities operated by Jones was fundamentally important.
3. The financial investigators are likely to have been particularly interested in any explanations provided by the account holder to the bank during the life of the banking relationship. Maintaining comprehensive and accurate records of such conversations is therefore important.
4. Institutions need to be particularly vigilant of the risks associated with cash intensive businesses and their appeal to local criminals. They should also ensure, during conversations with customers, that their tax affairs are up to date and all in order.

TYPOLOGY 2

UK resident using Jersey Bank Account to evade UK TAX – Attorney General exercises civil confiscation powers

In this case the Attorney General brought a representation to exercise his civil confiscation powers in December 2018, and the matter was then heard before the Royal Court and the Court of Appeal. In its judgment of 22nd July, 2019, (AG v Ellis [2019] JRC 141) the Royal Court found, after a contested hearing, that the account in question, which at the time contained £33,000, was tainted property. This was on the basis that the account holder had opened the account in the 1980s and had paid into it money from his legitimate taxi business based in Scotland, but with the intention of evading UK income tax on that income.

£42,500 entered the Account, and the respondent had failed to explain the source of those credits, despite being given opportunities to do so.

The respondent's solicitor had failed to provide evidence on his behalf, and indeed, had stated that the funds had been placed in Jersey for the purpose of tax evasion.

The amount currently contained within the account was significant and the respondent had taken no recent steps to establish the legitimate source of the funds or to obtain access to the money in the account.

Tax offences are generally triggered by events external to financial services businesses and very often as a result of internal transaction monitoring and media monitoring or in the case of Jones and Ellis being arrested for drug trafficking offences.

Generic Red flags - that a person may have been engaged in tax fraud include

- Approaches by customers requesting information to comply with a tax amnesty in their home jurisdiction.
- Secretive clients hesitant to produce tax advice when requested to do so or an unwillingness by them to discuss their tax status and/or their tax reporting.
- Participation in tax aggressive avoidance schemes often aimed at new high net worth individuals with a low understanding of the risks associated with such structures.
- A reluctance on the part of the client to confirm and provide evidence in relation to source of funds or source of wealth information.
- Conflicting accounts on the part of the client when clients are requested to provide information.
- Clients concealing their true income and failing to disclose such income to the bank and to the tax authority.
- Keeping business off the books by insisting that payment is made in cash and not giving receipts.
- Hiding undeclared income in complex corporate structures.
- Funds lying dormant with no clear explanation given as to why.

The following article examines the challenges faced by financial institutions when attempting to determine if they could be handling the proceeds of tax evasion – **https://www.jerseylaw.je/publications/jglr/Pages/JLR0102_the_difficulties_binnington.aspx**

The Financial Intelligence Analysis Unit (the "FIAU") in Malta has issued a helpful factsheet on typologies and red flag indicators of tax-related matter money laundering – **https://fiaumalta.org/news/fiau-factsheet-on-typologies-red-flags-indicators-of-tax-related-ml/**

TYPOLOGY 3

TAX EVASION – UK Case Study

The UK National Crime Agency secured assets worth an estimated £1.1 million, after an NCA tax investigation into a Derby man revealed that his family run business had avoided paying tax for 18 years, on profits suspected of being linked to drugs and other criminal activity. Tonino (otherwise known as Tony) Persico, 58, and members of the wider Persico family, operated ice cream vans and rented out industrial units on Osmaston Road.

A Derbyshire Police investigation looked at the family of Mr Persico after suspicions were raised about links to drugs, fraud, and money laundering, which resulted in the conviction of his sister for conspiracy to produce cannabis in 2013.

Acting on the suspicion that significant income had been generated through criminal conduct, the NCA adopted the functions of HMRC to investigate. This investigation determined that Mr Persico received rental and other income from industrial units in Derby and that a total of £1,135,857.82 of unpaid income tax, National Insurance payments, interest and penalties was payable for the tax years 1996/1997 to 2013/2014. Mr Persico did not respond to the NCA's claim and, on 1 November 2017, the NCA obtained a default judgment from the Court.

In the absence of any payment of the judgment from Mr Persico, the NCA applied to the High Court to enforce the debt against assets believed to belong to him. This was despite the fact that ownership of those assets involved various complex ownership structures. One such company was Osmaston Business Park Ltd, of which Mr Persico's niece became the sole shareholder at the age of 16. In the High Court the NCA alleged that Osmaston Business Park Ltd was, in fact, owned by her uncle, Mr Persico.

On 21 December 2021, the High Court handed down its judgment in this matter and granted the NCA a final Charging Order over the property located at 555 Osmaston Road.

In her judgment, Mrs Justice Foster DBE stated that the case

fell fair and square into the "concealment" category, that the true beneficial owner of the property was Tony Persico and she granted the Charging Order over the property in satisfaction of the tax debt. The NCA has already previously obtained Charging Orders over three other properties located at 555 Osmaston Road in which Mr Persico held an interest, in satisfaction of his tax debt.

https://www.wired-gov.net/wg/news.nsf/articles/NCA+set+to+recover+an+estimated+1.1+million+after+Derby+family+-failed+to+pay+tax+for+over+a+decade+24122021091000

Red flags

- Links to other types of criminality, drug trafficking etc.
- Complex ownership structure.
- Use of third parties close to the ultimate beneficial owner to conceal the true ownership of the property.
- Purchase of multiple properties as a means of laundering the proceeds of tax evasion.
- Failure of the person under investigation to provide explanations as to source of wealth and source of funds.

Learning points

1. The case underlines the importance of securing identification information of the true beneficial ownership of complex structures whilst mindful of the use of third parties to conceal the ultimate beneficial ownership of immovable property. TCSPs are expected to apply the three-tier test as set out in the JFSC document dated 20 August 2021 - https://www.jerseyfsc.org/news-and-events/beneficial-ownership-guidance-updated/
2. Collating identification details of shareholders of companies and keeping such information up to date is not only a legal requirement but also of considerable assistance to Law Enforcement conducting such investigations.
3. In conducting a risk assessment of Mr Persico, it would be important to consider the risks posed by other family members engaged in the family business, particularly Persico's sister following her conviction for producing cannabis.
4. Monitoring the transactions of the ice cream business and rental income from the industrial storage units could potentially ascertain whether other unlawful income was being intermingled with such revenue.

Drug Trafficking

Drug Trafficking Typologies

Banking
TCSP
Estate Agents
Lawyers and Accountants
Dealers in High Value Goods
Auditors
Money Services Businesses
Funds Services Businesses

Relevant to the following sectors – Banking/TCSP/Estate Agents/ Lawyers and Accountants/ Dealers in High Value Goods/ Auditors/ Money Services Businesses/Funds Services Businesses.

In 2020 the Jersey Financial Intelligence Unit ("FIU") received seventy three suspicious activity reports ("SARs") on the basis of the submitting institution suspecting drug offences. Drug users often resort to committing other crimes to fund their drug habit including the use of violence to enforce payment of drug debts. Drug traffickers in Jersey are usually part of a much wider organised and sophisticated drug trafficking networks based in the United Kingdom and Europe. The drug trade in Jersey mainly continues to be cash based, creating a dilemma for local drug dealers, namely what to do with the cash generated.

Drug Trafficking Typologies

TYPOLOGY 4

Drug Trafficking using the services of a local jeweller

Jersey Jeweller laundered the proceeds of drug trafficking for UK based organised crime group
https://www.jerseylaw.je/judgments/unreported/Pages/[2021]JRC182.aspx

Darius Pearce a Jersey jeweller laundered cash on behalf of a criminal enterprise that was engaged in the importation and supply of controlled drugs in Jersey on a commercial scale. He was convicted on 17th December 2020 following a 6 day Inferior Number trial and subsequently sentenced to seven and a half years in prison for money laundering.

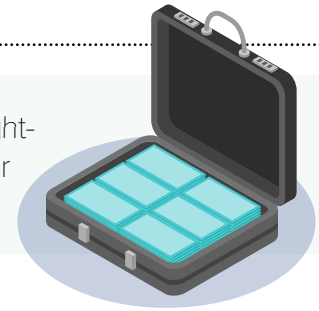
The case stemmed from a joint covert investigation conducted by the States of Jersey Police and the Jersey Customs and Immigration Service. The surveillance operation targeted numerous persons of interest and lasted several months. The operation culminated in the seizure of MDMA, cocaine and cannabis resin with a street value of up to £919,000, having been imported by boat at St Catherine's on 21 June 2019. The shipment of drugs was intercepted by law enforcement as it was landed, and all parties arrested. The covert operation also revealed the methods used by the gang to launder the proceeds from the drugs sold in Jersey.

The defendant responsible for laundering the proceeds of the drug trafficking was Mr Darius Pearce the director of Jersey Online Traders Limited, a Jersey holding company under which he was involved in several business ventures. One of those ventures was a jewellery business which the defendant ran from a shop in the Central Market in St. Helier, Darius Pearce Jewellers. The business had been in operation for many years.

Pearce used his jewellery business to facilitate the movement of criminal property from Jersey to the UK through the purchase and sale of gold bullion. This enabled cash to be removed from the Island under the cover of legitimate transactions, and without the cash being physically carried out of the jurisdiction, reducing the risk to the criminal enterprise that Law Enforcement intercepted and confiscated the cash.

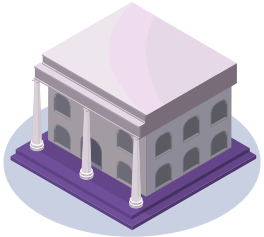
four simple steps

The process was straight-forward, effected in four simple steps



1 Firstly, a sum of cash would be handed to Pearce at his jewellery shop.

2 Secondly, Pearce would deposit that cash into his personal and business bank accounts.



3 Pearce would use the cash to purchase gold bullion from a dealer based in Hatton Garden in London.

4 The gold would be collected from the London dealer and sold for cash or retained as gold bars.

The cash or gold would then be available to UK-based members of the criminal enterprise to be used to purchase drugs, or otherwise to cover the operating costs of the criminal enterprise.

Pearce was convicted on three separate occasions of laundering money according to the steps set out above.

The total sum of money laundered was unknown but it was established that Pearce purchased gold bullion at a cost of £63,917.61 using criminal property.

Red flags

- Handling large volumes of cash, usually in high denomination notes. The drug trafficking trade in Jersey still uses cash as a means of purchasing and selling drugs but other methods are emerging including the use of prepaid cards and payment by Bitcoin. The sale of drugs creates a high demand for twenty and fifty pound notes.
- Erratic cash deposits from cash based businesses. Following a successful importation of drugs the cash generated is significant and organised crime groups will seek to intermingle the cash into the takings of a cash intensive business. A surge in cash takings, particularly if spread out at regular intervals may be indicative that the cash rich business is smurfing drugs money into its working capital. Such a modus operandi is becoming difficult to achieve given that businesses are increasingly resorting to the use of debit cards to receive payment particularly during the pandemic.
- Transferring money to the account of a third party located in the UK, without a plausible explanation. Money generated from drug sales must be removed from the jurisdiction to help fund the next importation. A pattern of transfers to third parties located in the UK could be indicative of drug trafficking.
- The use of multiple branches, multiple money services business and multiple payments through electronic money institutions, used to send money to third parties in the UK or globally.
- Regular deposits but under what the criminals perceive to be a reporting limit, for example multiple deposits or transfers of less than £10,000.
- Unexplained wealth of drug traffickers who are not in any meaningful employment.
- Attempting to convert the cash into high value goods for example jewellery, watches, cars and transferring the high value item to the supplier.
- Using the profits from drug trafficking to fund the purchase or part purchase of immovable property.

Learning points

1. The case highlights the importance of transaction monitoring, particularly in relation to cash deposits.
2. Clients who are uncooperative when challenged should be risk assessed accordingly.
3. The Jewellery business of Darius Pearce and indeed the case of Nat West Bank Plc, UK mentioned below highlights that long standing businesses are targets for organised crime groups keen to exploit the goodwill established with the business's bankers.
4. Monitoring the transactional activity of clients is key to assessing if the banking activity of the client has changed significantly. In October 2021 the JFSC published the outcome of its themed examination on transaction monitoring containing advice on best practice to consider. The full document can be located at **https://www.jerseyfsc.org/media/4938/20211022-transaction-monitoring-feedback-paper-web-final.pdf**

In October 2021 NatWest bank in the UK pleaded guilty to failing to monitor suspicious activity by Fowler Oldfield, a Bradford-based high street jeweller with a 100 year trading history of buying and selling gold, which deposited £365m over a five-year period, including £264m in cash. At the onboarding stage, revenue of £15m a year was anticipated, and it was agreed that the bank would not handle any cash. At its height however the bank was receiving £1.8m in cash a day. On the 13 December 2021 NatWest was fined £264.7m by a London court for failing to prevent alleged money laundering. The full details of the case can be accessed via the agreed statement of facts between the Financial Conduct Authority and National Westminster Bank Plc

https://www.fca.org.uk/publication/corporate/agreed-statement-facts-fca-national-westminster-bank.pdf

TYPOLOGY 5

Drug trafficking in relation to local organised crime

https://www.jerseylaw.je/judgments/unreported/Pages/%5b2021%5dJRC056.aspx

This typology represents a typical organised crime gang that on multiple occasions imported and sold class A drugs into Jersey and laundered the proceeds from the sale of the drugs.

> "The drugs were imported into the Island via the postal system but also via a courier"

Between 25th July, 2019, and 7th November, 2019, six postal packages were intercepted at Jersey Post Headquarters, all addressed to the place where Morgan was living with his stepfather. The subsequent covert investigation identified a drug trafficking gang engaged in the importation of class A drugs using a courier (Agathangelou) to bring the drugs from the UK to Jersey. The drug importations using a courier occurred on multiple occasions.

The laundering of the proceeds from the sale of the drugs occurred through the smuggling of cash out of the Island and the use of Bitcoin. Examination of Morgan's bank occurred revealed that he had made 12 payments to Bisson totalling £1500 for the purchase of heroin.

The drugs were imported into the Island via the postal system but also via a courier. In the case of Morgan, the Police examined his computer and were able to access a Bitcoin wallet showing incoming and outgoing transactions around the dates of the six postal packages. Morgan was stopped by Customs Officers when departing Jersey Airport bound for London and found to have £19,000 in cash in his suitcase which was subsequently confiscated.

Red flags

- Drug traffickers importing drugs into the Island continue to prefer the use of cash but are constantly seeking out new methods of converting the cash into a form that carries less risk of detection, for example Bitcoin.
- Using third parties to collect and carry the cash helps the drug dealer distance themselves from the proceeds of their crimes.
- Third parties are often targeted to carry the drugs because they themselves have a drug habit or have debts to clear.
- The proceeds from the sale of drugs are often required to fund the next drug shipment. Smuggling cash back to the drug supplier (usually located in the UK) involves a high degree of risk of detection by law enforcement at the borders. Such a risk acts as a powerful driver to seek out individuals or businesses willing to absorb such proceeds into their own banking facilities.
- Although no money services business was used in this case, any money services business operating in the Island is susceptible to being targeted by drug trafficking gangs keen to avoid the risks associated with carrying cash and preferring to send payment either directly to a supplier or to a trusted associate based in the UK.
- Drug dealers of class A drugs in the Island tend to collect a high volume of both Jersey and UK £50 and £20 notes due to the price paid for such drugs.
- In December 2021 the National Crime Agency announced it had arrested the alleged organiser for a £100m cash mule network smuggling cash out of the UK to Dubai indicating that cash still remains popular with organised crime groups in the UK.

https://www.policeprofessional.com/news/suspected-organiser-of-100m-cash-mule-network-arrested-by-nca/

To learn more about drug trafficking in Europe in only 120 seconds visit the Europol website
https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/drug-trafficking

Relevant to the following sectors – Banking/TCSP/Estate Agents/Lawyers and Accountants/ Dealers in High Value Goods/ Auditors/Money Services Businesses/Funds Services Businesses.

> "Online is the new frontline in fight against organised crime"

Fraud is increasingly being committed online. Where previously a fraud may have been committed by phone, post or in person, online access enables fraudsters to exploit victims remotely, often from another country. Some investment frauds, and most computer software service frauds, are known to be perpetrated from overseas. Online is the new frontline in fight against organised crime– says NCA on publication of annual threat assessment - National Crime Agency

Fraud is the most commonly experienced crime in the UK and globally. Fraud costs the UK many billions of pounds every year. The impact of fraud and related offences such as market abuse and counterfeiting can be devastating, ranging from unaffordable personal losses suffered by vulnerable victims to impacting the ability of organisations to stay in business.

Crime groups attack the UK public sector and government departments, such as the NHS, and billions are estimated to be lost to tax and benefit fraud each year.

See the latest fraud threat assessment from the National Crime Agency and listen to covert video clip entitled "How private is your personal information" to assess whether you are more vulnerable to fraud - Fraud - National Crime Agency

Fraud Typologies

TYPOLOGY 6

Where the fraud victims were known to the perpetrator

Managing Director of local financial services business convicted of fraud linked to a US based fraud.

Mr Byrne was the MD and founder of Lumiere Wealth Limited and an independent financial adviser who induced clients to invest in the Providence fund, a high-risk Guernsey based fund involved in factoring in Brazil. He did so by giving misleading assurances as to it being a 'safe' fund. He also concealed its high-risk nature and the fact that Providence was the majority shareholder in Lumiere Wealth and that he stood to benefit personally from investments into the fund. In one case he persuaded an elderly, poor-sighted, vulnerable widow to sign an agreement giving him an unsecured personal loan of £1 million by telling her she was investing the money

in a fund. In summer of 2016 the fund collapsed because it was a Ponzi scheme. It was not part of the prosecution case that Mr Byrne knew that the fund was a Ponzi scheme. Some of the investments were made whilst he did not have a licence from the Jersey Financial Services Commission ("JFSC") to provide investment advice. He provided false information to the JFSC regarding the loan during an inspection of his firm at which the offences came to light. Aggravating features were breach of trust; victims included both elderly and vulnerable clients; attempts to cover his tracks by forged documents on client files and false information provided to the JFSC.

Mr Byrne subsequently sold several properties to accommodate a confiscation order and partial compensation for victims.

Money received from victims in the Channel Islands was in part used to fund Lumiere Wealth Limited offices in Jersey and to support the lifestyle of the founders of the Providence fund Mr Antonio Buzaneli and Mr Jose Ordonez (both US citizens). The fraud in the Channel Islands was simply an extension of a virtually identical fraud perpetrated against US investors by the founders of the Providence Funds. Investors believed that they were investing into "factoring" in Brazil when in reality the majority of the money was siphoned off to support other ventures and the lifestyle of the founders and Mr Byrne. The publicly available filings from the Department of Justice revealed that the proceeds of the US fraud were used to fund a host of other companies linked to the founders, including an import/export company, a credit restoration service and even a catering company and food truck operated by Mrs Buzaneli. Funds from Channel Island Investors were used to help cover up the fraud being perpetrated in the US. **https://www.justice.gov/opa/page/file/1037296/download**

Christopher Paul Byrne **https://www.jerseylaw.je/judgments/unreported/Pages/%5b2018%5dJRC221.aspx**

Red flags

- Elderly and/or vulnerable clients being targeted and encouraged to invest life savings in high-risk products without understanding the risks involved.
- Movement of large volumes of a client's savings from a savings account and passed to a new start up business or to the personal account of their investment adviser – Such activity requires immediate contact with the Joint Financial Crimes Unit or The Financial Intelligence Unit.
- Jersey has seen some of the largest frauds committed by financial advisers misusing the information they have received in their capacity as an independent financial adviser. Such advisers are often very plausible, securing the absolute trust and confidence of the person being targeted. Whilst most independent financial advisers are honest and reliable, the rogue financial adviser often displays a combination of the following behaviours or adopts the following modus operandi.
- The fraudster arranges meetings with the person being targeted without a third person being present.
- The person being targeted is often retired or semi-retired with life savings providing low returns.
- The recruitment of a high profile or well-respected individual to provide an air of respectability to the product or company, for example securing a celebrity, politician or peer as a non-executive director.
- Encouraging clients to recruit or introduce other investors (family members) into the scheme through the use of a finder's fee.
- The fraudster recommends an investment in a high-risk product and misrepresents the risks or downgrades the risks when encouraging the client to invest.
- The fraudster deliberately omits to set out in writing the risks associated with the investment.
- The fraudster fails to explain how they themselves will financially benefit from the investment and that the fraudster has a direct financial interest in the recommended investment.
- The fraudster deliberately fails to produce documentation giving full details of the investment to the person being targeted.
- The fraudster discourages the victim to seek the advice of a third party before investing.
- The victim often refrains from seeking legal advice in relation to any loan agreement, at the advice of the fraudster.
- The victim often regards the fraudster as a friend rather than a professional financial adviser.
- Often the person being targeted has great difficulty in explaining what they have invested in.

Learning points

1. Providing financial advice whilst unauthorised to do so exposes investors to significant financial crime risks, including the risk of fraud.
2. Any investment adviser recommending a product to a client is required to undertake their own due diligence on the investment and in the case of the Providence funds such due diligence should have extended to the founders, Mr Buzaneli and Mr Ordonez.
3. Misrepresenting the level of risk to a client or seeking a loan from an elderly client to then invest into a high risk investment should be considered a significant red flag.
4. The JFSC issued a public statement listing all the learning points derived from this case which is accessible via **https://www.jerseyfsc.org/news-and-events/lumiere-wealth-limited-in-liquidation-lumiere/**

> “Fraud and falsehood only dread examination. Truth invites it”
>
> Samuel Johnson

Internet Fraud Typologies

TYPOLOGY 7

Detective Inspector
Aiden Quenault
JFCU Operations

The romance internet fraud. – Hypothetical case.

John joins multiple dating sites with a view to identifying and targeting vulnerable individuals seeking relationships. John operates from a jurisdiction with a poor law enforcement track record but uses technology to conceal his true whereabouts. He creates a false persona claiming to be a US military serviceman engaged in top secret work. On virtual calls he is seen wearing military uniform. Over a period of many months he carefully cultivates multiple relationships and slowly wins the complete confidence of his victims to the point where he begins to request that they loan him money to allow him to support a sick colleague or dying relative. He makes the first repayment as a means of ensuring that the next request for a greater amount is forthcoming. The requests for financial support become more frequent and for larger amounts. The victim is unquestioning of John's motive and obliges by sending him their life savings and is often persuaded by the prospect of moving to the US to live with John.

John successfully opens a company bank account in Jersey indicating to the bank that he buys and sells antiques online and the bank should expect payments from third parties. Once in receipt of funds he transfers the money to a company account he has control of. Both US companies were established several months earlier and operate from a virtual office. The name of the company is strikingly similar to a genuine business located in another jurisdiction. John quickly draws down the funds from the account through the use of a debit card and ATM machines. He remains cautious of keeping too much money in the bank accounts and his use of the ATM machines fluctuates with the number of victims he is able to defraud.

Victims start to become suspicious and exchange photos of John wearing military combat attire on the internet and contact their bank seeking advice on the recovery of money sent to John's account. Once detected on the internet the use of the bank accounts collapses and John creates another identity and seeks to secure further banking facilities.

Red flags

- Regular payments made by the same person or group of people, who appear unconnected to the account holder.
- Use of a virtual office facility.
- The age of the victim, usually with access to disposable income/funds.
- A newly incorporated company with little or no trading history operating a bank account.

Red flags

- The erratic drawdown of money via ATMs located in multiple locations.
- The creation of a false persona.
- The suspect is located in a jurisdiction with a poor law enforcement capability.
- The use of a false IP address to conceal the whereabouts of the suspect.
- Purporting to be employed within the military and using the same bogus photograph with several victims.

Learning points

1. The case highlights the important of securing KYC information from the client at the outset before operation of the account and taking steps to verify the legitimacy of the business.
2. Monitoring the account activity is likely to identify payments from third parties and the rapid draw down of funds using ATM machines.
3. The opening of any account on a non-face to face basis increases the money laundering risks and should be a factor when risk rating the client.

UK Bounce back loan scheme exploited.

The UK's National Audit Office estimates that the UK Treasury suffered an estimated £4.9 billion of fraud perpetrated through the UK bounce back loan scheme set up during the height of the pandemic. Prior to the pandemic the National Audit Office estimated that the level of fraud and error against Government was between £29.3 billion and £51.8 billion annually. The National Audit Office considers that figure to have grown substantially during the pandemic.

https://www.nao.org.uk/report/the-bounce-back-loan-scheme-an-update/?slide=1

TYPOLOGY 8

Bounce back loan fraud typology - UK case study

In 2021 two international fraudsters ran a £70m money laundering scheme in the UK, £10m of which originated from the UK Governments Bounce Back Loan Scheme. They have been jailed for a total of 33 years. **https://www.nationalcrimeagency.gov.uk/news/international-fraudsters-ran-70m-money-laundering-scheme**

Artem Terzyan, 38, from Russia and Deivis Grochiatskij, 44, from Lithuania, were the focus of a four-year investigation by the Organised Crime Partnership – a joint National Crime Agency and Metropolitan Police Service unit.

Their sentences are believed to be some of the largest ever handed down for money laundering in the UK.

Both men were also seen, along with other members of their criminal network, opening bank accounts in banks across London in the names of the various fake companies they had set up, then depositing tens of thousands of pounds into those accounts at a time.

The money would be sent from one shell company to another in a complex web of transfers, before it was sent out to international accounts held in countries including Germany, Czech Republic, U.A.E, Hong Kong and Singapore.

Grochiatskij's computer was seized from his flat. Officers discovered details of the bank accounts used by the pair for laundering, along with various incriminating photos of their

associates handling cash in Grochiatskij's living room on Grochiatskij's computer.

Another photo showed a safe containing a huge pile of cash.

While on bail, the pair began to exploit the Government's Covid-19 support scheme by claiming fraudulent Bounce Back Loans (BBL) for the various shell companies they had set up.

They claimed up to £50,000 a time, generating over £10m in total. £3.2m of that was claimed from one UK bank alone.

On top of this, they continued to launder criminal cash using the same method as before. Between June 2018 and November 2020, when the pair were arrested again, they laundered a further £34m including the £10m they generated from the BBLs.

Red flags

- Use of multiple fake shell companies with no trading history and poor credit rating.
- Significant use of cash.
- Making regular large deposits of ten thousand pounds into the bank accounts.
- Multiple claims of £50,000 being made at a time.
- Transferring the deposits into bank accounts operated in several overseas jurisdictions.
- Sudden surge in turnover on the accounts as the funding from multiple bogus bounce back loan applications were received.
- Organised crime group exploiting weak anti-fraud controls in place during a crisis.

TYPOLOGY 9

Where the proceeds have been used to support extravagant lifestyles or to support a failing business venture.

On 2nd July, 2018, the Superior Number of the Royal Court sentenced the defendant to a total sentence of imprisonment of 7 years for multiple offences of fraud, fraudulent conversion and falsification of accounts.

> "All three victims were elderly clients of a Jersey financial services business, who had placed complete trust in the defendant."

The total amount lost by the victims was £1,927,601. The frauds involved a trust established by a local resident, a company owned by a French resident, and a local resident. All three victims were elderly clients of a Jersey financial services business, who had placed complete trust in the defendant. The most serious offences related to the local resident whose trust was defrauded of some £1,768,601. The French resident's company was defrauded of £69,000 and the local resident was defrauded of £90,000.

Richard Arthur ("Mr Arthur") was a Chartered Accountant who at all material times was the Managing Director of a local accountancy firm that operated in Jersey.

The offences involved Mr Arthur persuading the victims to make a series of fraudulent loans from the funds held in the trusts/companies. In addition to the fraud offences Mr Arthur also pleaded guilty to falsification of accounts. Mr Arthur produced or caused to be produced a series of false accounts for the purpose of hiding from one of the victims the moneys which Arthur had fraudulently taken from the victim's family trust and its underlying company.

Mr Arthur pleaded guilty to obtaining and using for his own benefit the total sum of £2,637,401. The proceeds of the fraud were used to support a lavish lifestyle, support failing business ventures and repay disenchanted investors. In the subsequent confiscation proceedings, the prosecution realised assets from Mr Arthur's wine and art collection together with the proceeds derived from the sale of his substantial family home.

Red flags

- Lack of oversight by Mr Arthur's employers exposed clients to the risk of fraud.
- The lavish lifestyle of Mr Arthur did not raise enhanced scrutiny of his actions.
- Lack of challenge in relation to some of the transfers made to companies owned by or connected to Mr Arthur.
- Elderly and wealthy clients being targeted.
- The creation of false accounting records to conceal money transfers.
- Money being diverted to pay off debts.
- Funds used to purchase art and quality wines.
- Conflicts of interest not being effectively managed – Arthur was a director of Faircliff loaning monies to companies he beneficially owned, Solar GB Limited, Aqua Invest Limited.
- Lack of audited accounts.
- The person being challenged producing the accounts.

TYPOLOGY 10

Estate Agents – on the front line as criminals move to launder their money into property – Hypothetical case study

Real estate is as attractive to criminals as it is to any investor (especially here in Jersey with property prices continuing to rise). It is also functional, (as the property can be used as a second home or rented out, generating income. Real estate also provides a veneer of respectability, legitimacy and normality. This applies to both residential and commercial properties as part of a reliable and profitable investment strategy. Real estate transactions can involve large sums and are, in some jurisdictions subject to limited scrutiny with regard to money-laundering risks, when compared to other financial sector transactions.In Jersey property sales involve estate agents and lawyers thereby ensuring that SOW/SOF fund checks are applied with vigour.

> “Buying a hotel, a restaurant or other similar investment offers further advantages”

The use of real estate to launder money seems to afford criminal organisations a triple advantage, as it allows them to introduce illegal funds into the system, while earning additional profits and in some jurisdictions even obtaining tax advantages (such as rebates, subsidies, etc.).

The OECD reports that the three most common methods and schemes used by criminals are: price manipulation (escalating prices makes it easier to manipulate the prices of properties and transactions), undeclared income / transactions and the use of nominees and/or false identities, and corporations or trusts used to hide the identity of the beneficial owners - **OECD Report**

Real estate is commonly acquired in what is known as the integration or final phase of money laundering. Buying property offers criminals an opportunity to make an investment while giving it the appearance of financial stability. Buying a hotel, a restaurant or other similar investment offers further advantages, as it brings with it a business activity in which there is extensive use of cash.

The challenge is to spot the money laundering behind the real estate transaction. Possible indicators of money laundering (red flags) help the risk-based assessment. Guidance has been established as a tool for the sector at both global and national levels. More on this can be found in the European Parliament Briefing note which can be accessed via this link - **Understanding money laundering through real estate transactions (europa.eu)**

TYPOLOGY 11

Laundering the proceeds of crime through property purchases – Hypothetical case study

Mrs. X was a Director of a private hospital offering drug therapy treatment targeted at adults and children. To ensure her actions would go undetected she was also manipulating the procurement and payment systems of the hospital. The hospital received periodic donations from external donors for operations and upkeep. Mrs. X and her husband, Mr. Y set up a company and opened an account with a bank in an overseas jurisdiction. Mr. Y was recorded as a director of this company. When paying for supplies delivered to the hospital, Mrs. X submitted the account of her husband's company in the overseas jurisdiction and huge amounts of funds were electronically transferred into this account.

Using the funds from the hospital, the company bought a mansion in one of the affluent areas in the overseas jurisdiction along with several expensive cars. The property has since been seized through Mutual Legal Assistance Agreements between the two countries and the case is going through the courts.

Red flags

- Shell company – no seemingly legitimate reason for funds to be paid to this company, except to syphon off funds intended for the drug company and/or hospital.
- Multiple large wire transfers being paid in and out of a newly incorporated company.
- The use of cross border wire payments.
- Property purchased in a jurisdiction outside of where one of the owners was living and working.
- Purchase of high value property and goods, exceeding expected income.

TYPOLOGY 12

Mortgage Fraud – UK case study

The Serious Fraud Office ("SFO") began an investigation into a £50m fraud against mortgage providers. Following this investigation, the SFO secured guilty pleas against ringleader Saghir Afzal and chartered surveyor Ian McGarry ("Mr McGarry"), who was instrumental in the fraud.

The SFO's investigation showed how Saghir Afzal and his brother, Nisar Afzal, who fled to Pakistan before charges could be brought, defrauded a number of UK mortgage advisors into providing mortgages totalling £49,287,000 for properties worth only £5,688,125. They did this by recruiting a dishonest surveyor, Mr McGarry, to produce false valuations based on fictitious leases.

> "The way the fraud worked was similar in each case."

The way the fraud worked was similar in each case. A company controlled by the Afzal brothers bought a property, usually an old industrial building in a dilapidated state, from a genuine seller. The property was then bought and sold a number of times over a short period of time, each time for an apparently higher price. The only money that the Afzals paid out was for the initial purchase. This meant that when the final purchase of each property was completed the Afzals obtained a huge "profit" by virtue of receiving the fraudulent mortgage loans. After making one or two early mortgage payments, the companies controlled by the Afzals stopped paying the mortgage and the Afzals disappeared with all the money. This left the lenders to try to recover their losses by selling the properties following repossession. It was then that the lenders discovered that the properties were worth only a fraction of what they had lent, in some cases as little as 10% of the monies advanced.

Mr McGarry accepted bribes from the Afzal brothers totalling over £1m, including lavish overseas holidays in Dubai, an Aston Martin car, cash in brown paper envelopes and the purchase of three properties in London. In return he prepared inflated valuations for each property which the lenders relied on when advancing the mortgages. In one instance Mr McGarry valued a property at £19m that had been purchased for just £1m. This represents an overvaluation of 1800%. In another instance, McGarry produced three different valuations of the same property, on the same day, for three separate financial institutions.

Saghir Afzal was sentenced to 13 years' imprisonment and Mr McGarry was sentenced to seven years' imprisonment. Saghir Afzal was also ordered to pay a confiscation of £29,276,565 within six months and was sentenced to an additional ten years' imprisonment for his failure to do so. Mr McGarry was ordered to pay £1,549,447.95, which he paid in full. Click on this link to read the SFO report into this case in full - **Birmingham Mortgage Fraud - Serious Fraud Office (sfo.gov.uk)**

Red flags

- The lavish lifestyle, overseas holidays in Dubai, high end vehicles of those involved in this fraud.
- The use of excessive cash payments.
- The purchase of three London properties, source of funds and wealth.

Learning points

1. Mortgage lenders should undertake independent checks to validate the true price of the property.
2. There is a risk in accepting documents at face value.

TYPOLOGY 13

Money Laundering - laundering the proceeds of people trafficking by purchasing a restaurant. – Hypothetical case study

Mr X purchased a restaurant that he had financed by a mortgage at Bank A. The restaurant was subject to a lavish and costly makeover. Mr X owned a chain of restaurants across the UK one of which was raided by the Border Force officers and featured in local media reports suggesting that the premises were employing illegal migrants. Accommodation attached to the restaurant was used to offer a high class escort service. A local estate agent facilitated the sale of the restaurant. The mortgage was repaid within two years by transfers from an account opened with Bank B in the name of his spouse and located in another jurisdiction. Within two years his spouse's account was credited by cash deposits and debited by cash withdrawals, as well as transfers to Bank A effectively clearing the outstanding mortgage.

When asked for evidence as to source of funds and source of wealth by the estate agent handling the purchase of the restaurant Mr X initially claimed that the funds were generated from other business interests but was unable to produce evidence to support his explanation. When challenged he became evasive often changing his account.

Debits on the Bank B account also revealed various transfers to Cambodia in favour of a natural person. Intelligence indicated that Mr X was part of network that facilitated the entry of illegal migrants from Asia into the UK and then used as slave labour in the catering trade.

Red flags

- The rapid and unexplained repayment of a mortgage facility.
- Cash deposits and cash withdrawals.
- Funds received to pay off the mortgage received from the account of the spouse located in another jurisdiction.
- Operating an escort service possibly using victims of people smuggling.
- Changing explanations provided as to source of funds and source of wealth.
- The purchase of a restaurant could provide Mr X with the opportunity to smurf the proceeds from people smuggling and the legitimate earnings from the business into the banking system.
- Transfers to a natural person in Cambodia could be indicative that payment was being made to fund the lucrative people trafficking operation and pay the person recruiting victims.
- Mr X owns a property that has been associated with employing illegal immigrants.

To complement this typology, other features can serve as specific indicators of real estate money laundering, such as:

- recourse to third parties by customers (sellers and buyer) for concealment of ownership.
- unusual income (e.g. no income, or inconsistency between income and standard of living), unusual rise in financial means, unusual possession or use of assets, or unusual debt (e.g. mortgage with low income or unidentified lender) on the part of the legal owner.
- use of front companies, shell companies, trusts and company structures, allowing the criminal not to appear as the real owner.
- rental income to legitimise illicit funds (either with rental funds provided by the criminals for the tenants to legitimise illicit funds, or renting the property to a third party they use as the legal owner);
- property renovations and improvements using illicit funds that increase the value of the property, which is then sold at a higher price.
- property developers appearing to pay over the top prices for land or property for development/redevelopment
- consideration of geographical elements.

Money laundering through real estate is much harder when the required checks are robustly undertaken on the owner of the property, the source of funds and their overall wealth. For more information on this typology click on this link to a paper published by Transparency International - **Three ways to stop money laundering through real... - Transparency.org**

Money Laundering
in the securities sector

The securities industry plays a key role in the global economy. Participants range from multinational financial conglomerates that employ tens of thousands of people to single-person offices offering stock brokerage or financial advisory services. New products and services are developed constantly, in reaction to investor demand, market conditions, and advances in technology. Product offerings are vast, and many are complex, with some devised for sale to the general public and others tailored to the needs of a single purchaser. Many transactions are made electronically and across international borders.

TYPOLOGY 14

Redeeming a long-term investment within a short period – Hypothetical Case study

A customer Mrs X who has been known to the bank for some time meets with her Independent Financial Advisor (the "IFA") with a view to placing a large sum into an investment product. During the meeting Mrs X provides the IFA with all the CDD documentation requested. As this is a known customer, who is rated as medium risk, no enhanced due diligence is requested from her. The source of her funds is a recent wire transfer received in from her husband's personal account held at another bank. She tells the IFA that this is his annual bonus payment, which he has gifted to her, and the IFA can see that she has received other smaller payments in from her husband's account over the last 12 months. The meeting goes well, the customer signs the paperwork, and her investment into her chosen fund is completed. However, within less than 18 months of taking out the investment Mrs X instructs her bank to sell her holding in the fund. She advises her bank that she is aware that as a result of this action she will incur a small loss. As part of the banks surrender procedures, a call is made to the customer to ask for the reason for closing out of this fund early, and she says that it is to pay medical expenses. As she is still rated as medium risk no further enquiries are made. Her holding in the fund is redeemed and the funds are transferred into her account. Within days, a similar but smaller amount is transferred out to an unknown third party in an overseas jurisdiction.

The husband of Mrs X is subsequently arrested and charged with fraud and corruption. Research indicates that he has also in the past been convicted of tax fraud. Has Mrs X successfully laundered funds through this fund and her bank account?

Red flags

- The receipt of the instruction to redeem her holding from the fund should have prompted further questioning and a review of her risk rating.
- Is this an indication that this customer is in some financial difficulty?
- Transaction monitoring should have picked up the rapid payments made, prompting further questioning.
- Source of funds and wealth. What is known in regards to her husband's business activities and his past?
- Suspicions relating to the early redemption of funds should prompt further questioning of the customer, if no satisfactory explanation is given for the unusual activity a SAR should be submitted to the MLRO.

Learning points

1. Suspicious activity reporting for this sector remains relatively low, when compared to Banks and TCSPs. This could be due to a lack of awareness of the SAR reporting requirements and it is important that employees working in this sector continue to receive regular and specific training which includes securities-specific indicators and the use of case studies.

Other key points to look out for in this sector are:

- Securities accounts introduced from one intermediary to another without adequate customer due diligence/know your customer (CDD/KYC) investigations or from high risk jurisdictions.
- The use of front persons or entities (e.g. corporations, trusts).
- Entities with complex corporate structures.
- Politically-exposed persons (PEPs).
- Dealings with financial institutions and intermediaries or customers operating in jurisdictions with ineffective AML/CFT systems.
- Unregistered or unregulated investment vehicles.
- Cross-border omnibus and correspondent accounts.
- Fictitious trading schemes.
- Changing share ownership in order to transfer wealth across borders.
- Opening multiple accounts or nominee accounts.
- Using brokerage accounts as long term depository accounts for funds.
- Effecting transactions involving nominees or third parties.
- Engaging in market manipulation, e.g. "pump & dump" schemes.
- Engaging in boiler room operations, targeting vulnerable clients.

More information relating to this sector can be viewed on the FATF website - **ML-TF vulnerabilities of the securities sector (fatf-gafi.org)**

Relevant to the following sectors – Banking/TCSP/Estate Agents/Lawyers and Accountants/ Dealers in High Value Goods/ Auditors/Money Services Businesses/Funds Services Businesses.

TYPOLOGY 15

Corruption – Laundering the proceeds into Real Estate

X is a successful politician in a developing country and receives bribes in order to allocate lucrative government contracts. He sets up three overseas companies. To hide his involvement in the companies he uses a close business associate to act as the covert beneficial owner of the companies. The companies are administered by a Trust Company Service Provider (TCSP). The TCSP appoints a legal representative to incorporate the companies and execute the purchase. For each of the companies, the TCSP opens a bank account with three different banks in different jurisdictions. The individual uses the three companies to set up a loan-back scheme in order to transfer, layer and integrate the proceeds of the corruption. He then co-mingles the criminal funds with the funds that originated from the legal activities of one of his companies. Next, the third party purchases a substantial property for the use of X using the services of an estate agent. The third party indicates to the estate agent that due to work pressures he was unable to visit the property before making the purchase but is prepared to make an offer for the property over the asking price if necessary. No mention is made of X to either the estate agent or the lawyer facilitating the purchase of the property. To finance the transaction, he arranges for a loan between two of the companies both of which were domiciled in the Caribbean. The property is then settled into a charitable trust administered by the TCSP.

Red flags

- PEP relationship involved in companies banking in overseas jurisdictions - again this should be reflected in the risk assessment
- The source of the funds used to finance the real estate transaction was from overseas
- The lender of the money, an offshore company, had no visible link to the borrower of the money.
- The loan agreement in place was poorly drafted and had not been produced by a legal professional.

Red flags

- The poorly constructed loan agreement was legally invalid.
- The information in the loan agreement was inconsistent or incorrect.
- The conditions in the loan agreement were unusual (for example, no collateral was required).
- No payment of interest or repayment of the principal amount featured in the loan agreement.
- The purchaser did not wish to view the property.
- The purchaser was prepared to pay over the asking price.
- The Ultimate Beneficial Owner of the property is a PEP and therefore high risk. His link to the purchase of the property is concealed from the Estate Agent and Lawyer.
- The use of a third party to covertly undertake the purchase and hold the property on behalf of the ultimate beneficial owner is a strong indicator of money laundering.

TYPOLOGY 16

Corruption – Windward Trading Limited

In 2016 a Jersey company, Windward Trading Limited ("Windward Trading") pleaded guilty to four counts of money laundering offences involving a total of £2,599,050 and US$2,971,743 respectively acquired or possessed by Windward Trading between 29th July, 1999 and 19th October, 2001. The company received and held the proceeds of criminal conduct perpetrated by its controlling mind and beneficial owner, Samuel Gichuru ("Mr Gichuru"). The company knowingly enabled Mr Gichuru to obtain substantial bribes paid to him while he held public office in Kenya. The company played a vital role without which corruption on a grand scale would not have been possible.

Mr Gichuru was the chief executive of Kenya's power utility, the Kenya Power & Lighting Company ("KPLC") from November 1984 until February 2003. He accepted bribes from foreign businesses that contracted with that company during his term of office and hid them in Jersey. Payments were made to third parties one being to a former minister in the Kenyan government and another to a former head of public service in Kenya.

Windward Trading is now administered by a completely new trust business, which acquired a trust company book of business including Windward Trading from a Jersey Trust and Company Service Provider (TCSP) who in turn had acquired the responsibility of providing services to the company following its acquisition of another Trust and Company book of business in 2007. The original TCSP had in May 2002 filed a suspicious transaction report and from which point the affairs of the defendant company were effectively frozen.

Windward Trading pleaded guilty to money laundering and funds held by the company were subject to a forfeiture order by the Royal Court.

The Attorney General continues to seek the extradition of Mr Gichuru from Kenya. **AG-v-Windward Trading Limited 24-Feb-2016 (jerseylaw.je)**

Red flags

- Mr Gichuru was a PEP and therefore the relationship was high risk from the outset.
- Money was received by Windward Trading and paid to third parties without adequate challenge.
- Bribe payments were received into the company account and then paid to prominent individuals holding high office in Kenya.
- The account was first opened in 1981 and it is therefore important to review the operation of legacy business accounts.
- The timely submission of a suspicious activity report can prevent the dissipation of the proceeds of corruption.

Relevant to the following sectors – Insurance/dealers in high value goods/Banking.

Insurance products, like other products offered by the financial service industry, are at risk of being used as money laundering vehicles. Most financial institutions will view wire transfers, originating from insurance companies, as medium to lower risk payments, due to the level of due diligence applied by the insurance company at on-boarding. In some countries, insurance activity is operated cross-border, and the products are sold through brokers or intermediaries, who may not be under the supervision or control of the insurance company who owns the product. This could potentially make these products more attractive to money launderers, due to the additional layers involved in the process. Suspicions of money laundering connected to the insurance industry and/or products need to be reported to the FIU as a suspicious activity report.

TYPOLOGY 17

Money Laundering using Insurance Claims

Mrs C purchased marine/motorboat insurance for her large cruiser. This covered the loss/damage of her ship, the hull including machinery and its equipment, passenger liability, personal property and any valuables on board, its crew (personal accident and medical cover), its cargo, the use of terminals, tenders, etc. She used the services of a broker, not dealing with the insurance company direct. Through her coercion of the broker, the ownership documentation was accepted and certified and no independent validation was undertaken to confirm that she owned the vessel. She ensured that she regularly paid the large premiums due, initially making some over payments and some payments in cash. Others were made by wire transfer, and they were always made on time. However, over a number of years she was able to make regular and varied claims through her broker, all of which were accepted and paid out, with little or no challenge. These claims, although they appeared to be frequent in nature, totalled less than the overall premium payments made, and as such they did not attract attention, as the insurance company was still benefiting from the policy. Using this technique her money was effectively being laundered over a number of years, and the fraudulent claim payments were transferred directly into her bank account. As these wire payments originated from a reputable insurance company and were not considered to be of a high value, they were not subject to enhanced scrutiny or to additional questions around the source of her funds.

> “no independent validation was undertaken to confirm that she owned the vessel.”

Red flags

- The purchase of an insurance policy and then making a claim soon after could potentially highlight a concern.
- Numerous or frequent claims or pay outs, which when looked at in totality, appear suspicious.
- The use of cash or cross-border wire payments for large premiums, source of funds.
- Why are overpayments made when the premiums are already large?
- Frequent payments into the bank account from the insurance company, source of funds.
- The risk of placing reliance on a third party to undertake customer due diligence and the validation of the property being insured.

Learning points

1. The use of cash for any premium payments should be considered suspicious and an attempt to place criminal funds into the financial system.
2. Questions should be raised when over payments are received.
3. Encourage the use of boat registries to independently validate ownership.
4. Further questioning should have been completed around the customer's source of funds and overall wealth; this could have highlighted concerns around the legitimacy of the insurance policy.
5. Regular training, vetting and oversight over brokers/intermediaries, and their adherence to comply with the insurance company's AML policies and procedures.
6. Scrutinising the claims made in totality rather than singularly.

The Financial Action Task Force ("the FATF") has produced a report on money laundering typologies in the insurance sector. To read more about this topic click on the following link - **Microsoft Word - TY2004_en.doc (fatf-gafi.org)**

> "Corruption is a cancer, a cancer that eats away at a citizen's faith in democracy, diminishes the instinct for innovation and creativity."
>
> Joe Biden

Relevant to the following sectors – Investment business/ banking

Insider dealing has been a criminal offence in the UK since 1985. It occurs where an individual trades shares or securities using material, non-public information, acquired or obtained, which is price sensitive. The material or information is not available publicly and is likely to affect the share or trading price of the company concerned. This individual may or may not be an "insider" of the company to which the information relates but has acquired non-public information and goes on to use that information to gain an unfair advantage, by either buying or selling shares. The aim of this is to acquire a personal gain, ahead of the "inside" information becoming publicly available. While the rules governing insider dealing are complex and vary between jurisdictions, it is considered to be illegal activity in most countries, including Jersey, and the transfer of the proceeds into a bank account should be considered money laundering and reportable via a suspicious activity report to the FIU.

TYPOLOGY 18

Typical Insider Dealing Case Study

Mr A is a senior manager of a large retail company and, given his position, he is made aware that a restructure of the retail group's headquarters is going to be publicly announced over the following week. Ahead of this announcement he meets with his brother Mr B for dinner, and over coffee he confides in his brother, telling him the high-level details of the impending restructure. They part planning to meet up again over the next few weeks, and Mr B starts to reflect on the conversation he has had with his brother and the non-public information he shared with him about the changes being made to the retail group. He is aware that this announcement is due to be made in the following week and is also aware that once the information becomes publicly known it is likely to have a favourable impact on the share price of the group. Mr B acts on this insider information and instructs his broker to purchase a significant shareholding in the retail group that his brother works in, ahead of the announcement of the restructure being made to members of the press and the public.

Once the restructure is announced, the share price of the retail group, as he anticipated, rises significantly. Mr B then instructs his broker to sell his shares making him (Mr B) a considerable profit. The funds from the sale of his shares are then transferred by his broker into his bank account as a wire payment. As the profit from the sale of the shares has been obtained illegally, using material non-public information to gain an unfair advantage, the payment made has been laundered through the transfer to his bank account.

Red flags

- The customer has acted on material non-public information.
- The customer is known to have a close family member working at the company impacted by the news/announcement.
- The purchase of a large number of shares in a company shortly before a significant announcement is made, which favourably affects the share price, could indicate insider dealing.
- The customer's purchase does not correspond to his investment profile. For example, the customer hasn't previously invested in shares in this retail group, but has done so at what appears to be an opportune time.
- The customer's bank account is opened or significantly funded shortly before the share purchase.
- The customer sells his shares following the announcement, making a clear profit for himself.
- Both brothers are potentially guilty of insider dealing. Mr A should not have divulged this sensitive information to his brother, and Mr B should not have acted on the information given to him.

Learning points

1. It is illegal to share material non-public information with anyone who is not considered to be on the "insider list" and subject to the company's controls established around the material non-public information
2. Companies should have a clear policy on handling material non-public information and insider dealing
3. Regular and effective training should be given to all employees who have access to or who are handling material non-public information, and the risk of committing the offence of Insider dealing
4. It is illegal to act on material non-public information to gain an unfair advantage in the marketplace.
5. All Brokers should remind their customers of the risk of the insider dealing offence
6. Most Brokerage companies and banks have surveillance tools in place to identify instances of insider dealing
7. The main regulatory provision is contained in Part 3A of the Financial Services (Jersey) Law 1998, which closely follows the rules contained in the UK's Criminal Justice Act 1993 and the Financial Services and Markets Act 2000. A person found guilty of insider dealing or market manipulation is liable to imprisonment not exceeding ten years or an unlimited fine.

The FATF has produced a publication setting out risk factors in laundering the proceeds of crime from insider dealing.
To read more about this topic click on the following link - **ML-TF vulnerabilities of the securities sector (fatf-gafi.org)**

> "Defeating human trafficking is a great moral calling of our time."
>
> Condoleezza Rice

Terrorism

Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse.

TYPOLOGY 19

Terrorism Hypothetical Case Study

Client X portrays himself as a successful entrepreneur from West Africa with a vast business empire specialising in the commercial production and export of charcoal to the Middle East and more recently diversifying into the extraction of high value minerals again in East Africa. Client X is introduced to a Jersey Trust and Company Service Provider ("TCSP") with a view to incorporating a Jersey company to purchase a significant property in London and settling the asset into a tax efficient structure. Client X also seeks to settle funds into a trust structure to fund the education of his children. As the relationship with the TCSP develops further, Client X seeks to incorporate Jersey companies to manage new business ventures in Africa, including road haulage and shipping. Client X regularly pays the feared terrorist group Al-Shabaab a tax for all charcoal and minerals exported. In addition, he pays protection money to Al-Shabaab to ensure that his road haulage and shipping assets remain free from interference. In short, client X through his trading companies helps fund the terrorist activities of Al-Shabaab.

To learn more about how the charcoal trade provides support to terrorist groups like Al-Shabaab read the 2020 Interpol publication "World Atlas illicit Flows"

World Atlas of Illicit Flows | Zoï Environment Network (zoinet.org)

Red flags

- The client is associated with a high-risk jurisdiction.
- The TCSP is providing services to a trading company.
- The charcoal trade is a known source of funding for the Al-Shabaab Group.

Learning points

1. The Jersey TCSP needs to conduct a comprehensive risk assessment of client X at the onboarding stage including his business activities.
2. The geographic risk associated with the business activities of client X must form part of the client risk assessment.
3. Interviewing the client as part of the onboarding process is likely to be key.
4. Referring the onboarding decision for client X to senior management or to a committee dedicated to reviewing the risks associated with onboarding high risk clients is recommended.

TYPOLOGY 20

International Terrorism Hypothetical Case Study

Client A has a long-standing banking relationship and unremarkable banking history. Since retiring from the armed services on medical grounds he has dedicated much of his time to supporting a far-right wing extremist group ("the Group") and regularly raises funds for the Group by way of selling memorabilia and organising training sessions for members in remote locations. Such training includes weapons training and bomb making skills. The Group advocate violent direct action against any organisation that helps to support illegal migrants into the country. In recent times, the Group have focused their attention on community leaders and politicians seeking to intimidate and drive their agenda. Client A uses his bank account to receive third party payments for the sale of the memorabilia and attendance at the weapons training events. Payments are made to hire venues for the training events. He also posts pictures of himself wearing paramilitary clothing and carrying a firearm advertising the next training session. The volume of third-party payments into a personal bank account causes concern at the bank. When challenged by bank staff, client A claims that the funds received from third parties represent income derived from trading on eBay. Client A is subsequently arrested at a violent demonstration and charged with violent disorder and the unlawful possession of a firearm with intent to endanger life resulting in a media report describing him as the treasurer of a far right wing extremist Group.

Red flags

- Change in banking activity.
- Unexplained third party payments being received regularly.
- The photographs posted on the website.
- Payments made to secure training venues.
- Client A concealing the true reason for the third-party payments.

Learning points

1. Research indicates that far right-wing extremists have enjoyed a significant increase in popularity during the Pandemic.
2. Selling marketing material, music and attendance at training camps act as a valuable source of funding.
3. Undertaking internet research as part of the onboarding process AND ongoing monitoring should enable the bank to identify the emerging risks as Client A becomes more extreme in his views and behaviour.

To learn more about how far right extremist terrorist groups fund their activities visit the below link.
https://www.fatf-gafi.org/media/fatf/documents/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf

“Money is the life blood of any terrorist organisation and anyone who makes property available to a terrorist organisation helps that organisation further its objectives of murder and destruction.”

Mr Justice Hart

in sentencing remarks for a Real IRA terrorist convicted of financing a weapons purchase plot.

Gun plot RIRA man sentenced to 20 years - BelfastTelegraph.co.uk

Government of JERSEY

Produced by Baker Regulatory Services Limited.

“Money laundering is not a victimless crime and the ramifications of ineffective action are real.

Failing to take action means organised criminals trafficking people, drugs, arms and wildlife, and corrupt stakeholders and terrorists, operating with impunity”

FATF