Bailiwick of Guernsey
Financial Intelligence Unit

STEP GUERNSEY

Guernsey Branch Conference 2024

FIU Update – Emerging Risks/Threats

Adrian Hale

Head of FIU

Bailiwick of Guernsey
Financial Intelligence Unit

1. Statistics 2023 / 2024
2. FIU Core Functions
3. Common Trends / Threats
4. Understanding Fraud and Scams
5. Private Public Partnership Update
6. What is a Money Mule?
7. Risk of Sextortion

FIU Statistics (2023)

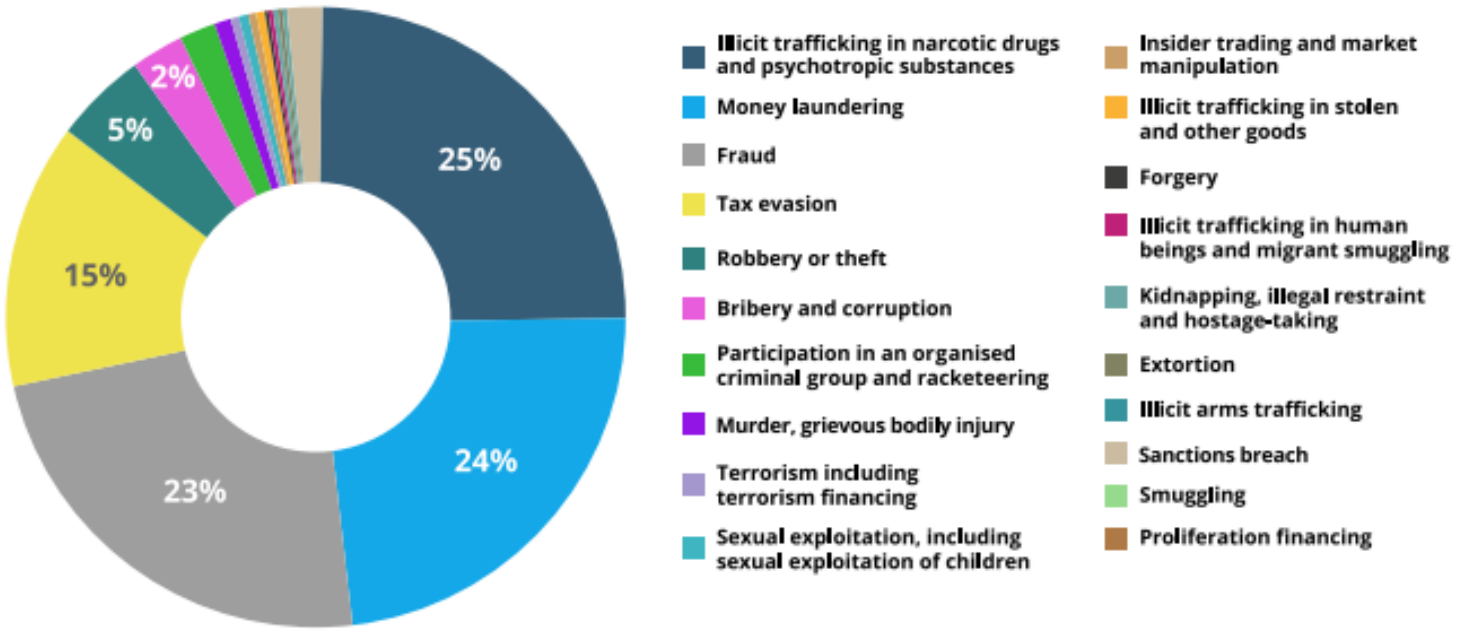


Figure 4: Pie chart showing the percentage of SARs in 2023 per suspected criminality

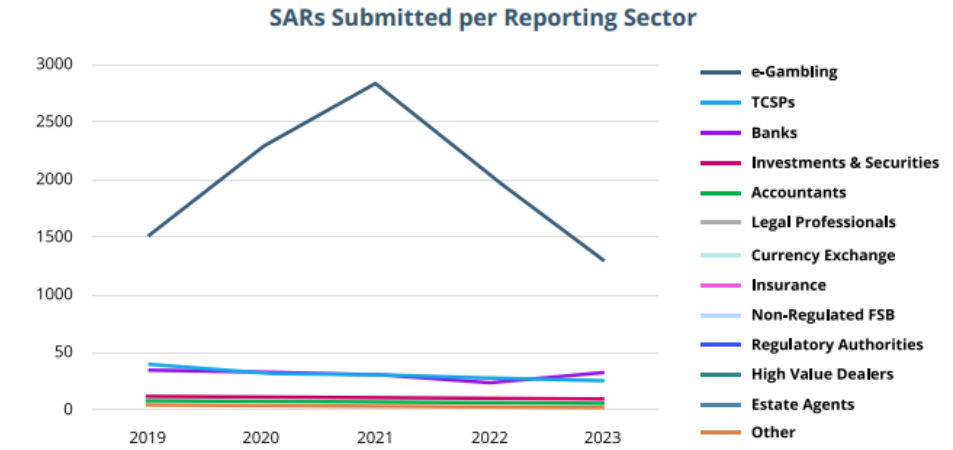


Figure 2: Line chart showing a count of SARs submitted per reporting sector

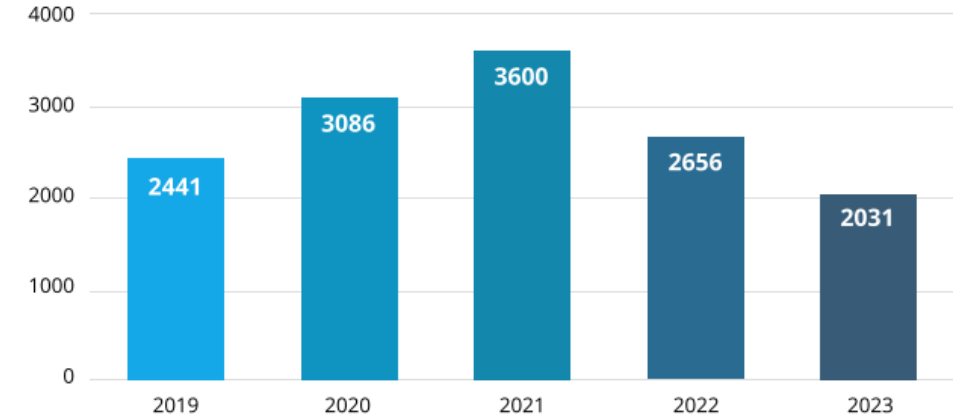
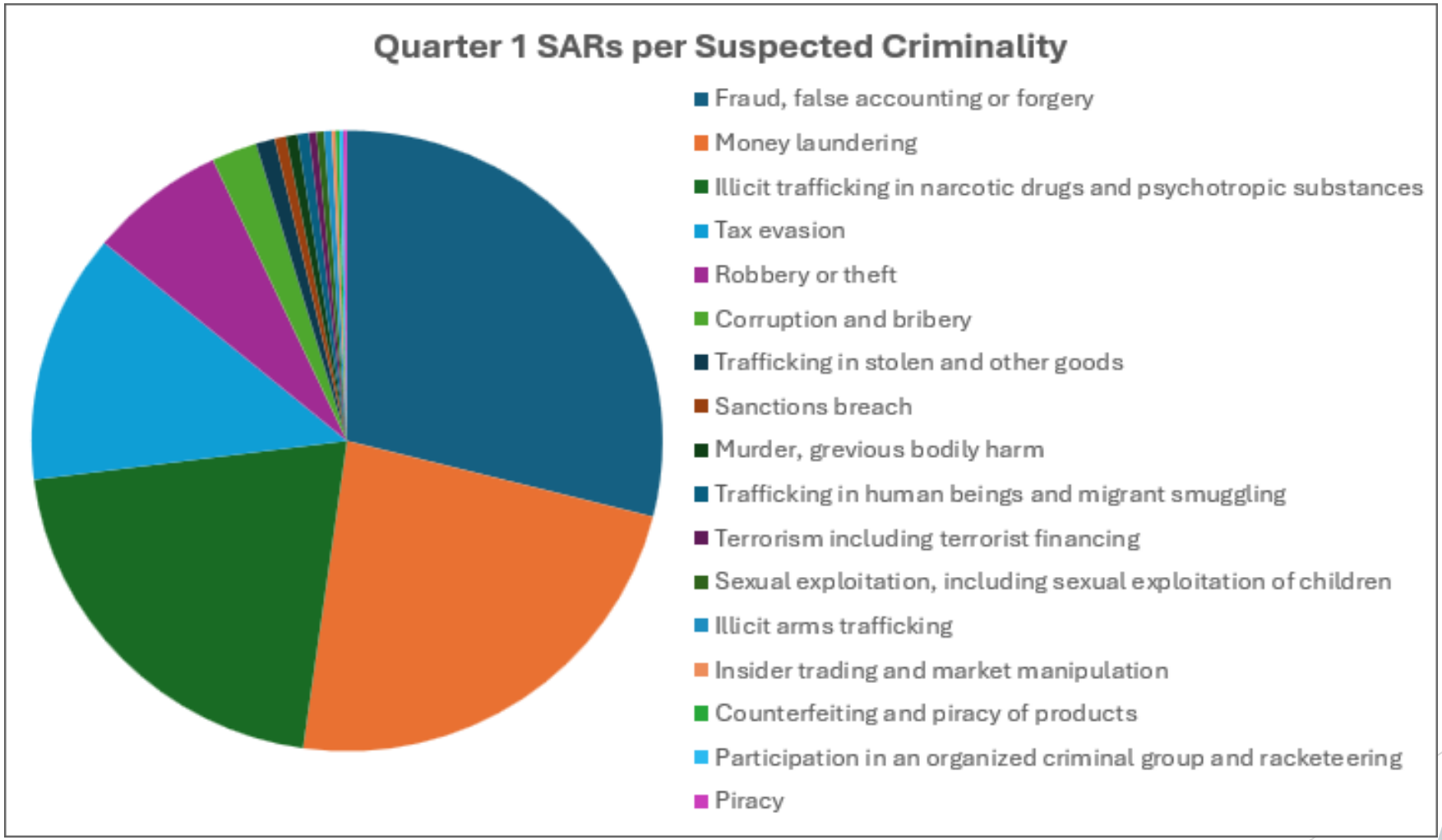


Figure 1: Column chart presenting the number of SARs submitted to the FIU per year

FIU Statistics (1st Quarter 2024)



FIU Core Functions

- FIU Core Functions – prescribed under the FIU Law and in compliance with the FATF International Standards – Recommendation 29
- Operational Analysis – Identify specific 'Targets', ID proceeds of crime, money laundering, terrorist financing and proliferation financing
- Strategic Analysis – Use all available information (data etc.) to identify ML, TF and PF '***Trends***' and '***Patterns***'
- Emerging '***Risks***', '***Threats***, '***Trends***' and '***Patterns***' i.e. Russia/Ukraine, Cyprus Papers, Bailiwick's NRA, SAR Analysis
- What are we seeing?
- Increase in SARs – Fraud, attempted fraud, money mules, decrease in SARs from specific sectors i.e. TCSPs, Estate Agents
- What are we doing to prevent these '***Risks***' etc?

Understanding Fraud and Scams

Q. What is the difference between a fraud and a scam?

A fraud

is the theft of a victim's money without their knowledge or permission.

- Debit or Credit Card Fraud
- Bank Account Takeover
- Identity Theft

A scam

is the theft of a victim's money with their permission or knowledge.

- Shing scams, Phishing (emails) Vishing (phone calls), Smishing (SMS or e-messages)
- Impersonation or trusted source scams
- Investment scams
- Romance scams
- Purchase scams

How to Spot a Scam

It can be hard to spot fraud and scams, however, there are some tell-tale signs to look out for:

1. Have you been contacted out of the blue? Were you expecting the call or email? Are you being asked to make an unexpected payment or to disclose personal or banking details?
2. Have you been sent an attachment or a web link, and told to take urgent action?
3. Have you been contacted by a supposedly trusted source, such as your bank or the police? Are you being pressured to take action? Have you been told to lie to your bank if they call you to validate a payment?
4. Is it too good to be true? Are you being offered excessive returns on an investment or crypto? Is the sales price far cheaper than a comparable product or service?
5. Is there a sense of urgency or pressure to act, to disclose personal or banking details, to make a payment?

Advice & Guidance

Never send money to someone you have not met face to face and whom you know well. Emotional and manipulative language will be used to trick you into sending money for a cause or reason that does not exist.

When dating online, always use a trusted and reputable dating app or website as their chat function will contain filters designed to identify fraudulent and scamming language and terms. Always keep your conversations on the app or website and never be persuaded or pressured into moving to another chat service.

Never invest, into crypto or precious metals, following advice you have been given through a dating app. You have no way of verifying the person as a qualified, experienced or legitimate investor, and, you will often be asked to transfer money, assets or holdings to them to "manage on your behalf", which you will never see again.

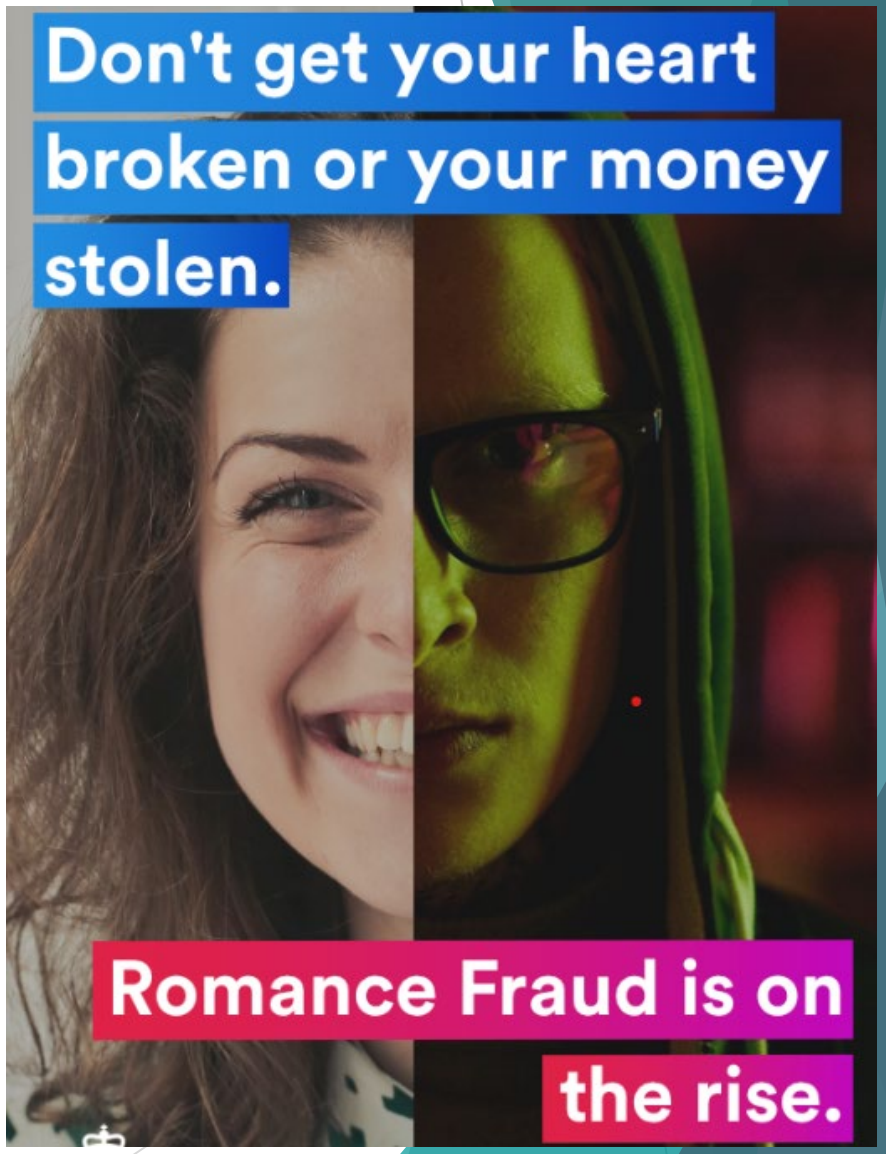
Compromised Email Fraud

- Trust & Company Service Provider (TCSP) maintain a relationship with Business A – UK National – Textile Business
- Regular Payments to various countries, circa £300k
- Email adrianhale@icloud.textileworld.com
- Business A communicating with TCSP via encrypted line
- Multiple emails concerning number of incoming requests for payments
- Payment to Company X, Hong Kong, Reference textile purchase
- Payment $1.3 million confirmation email received adrianhale@icloud.textileword.com
- Payment authorised and paid
- Secondary check with client – unauthorised payment
- Contact the FIU immediately – Why?
- Speed is of the essence – Why?

CEO Fraud – How it Impacts You

Romance Fraud

- A customer wishes to post money to Mr X in UK or foreign country
- Explains that they met Mr X on internet
- Mr X needs money to travel to Guernsey
- Initial £100, then £200 ++++
- Customer background (vulnerable, age, and background!!)
- Final £2k payment
- Plain clothes Police engagement
- Result – Preventative measures



Preventing Fraud – What To Do

Always keep your full card details safe and secure and never disclose your details freely. Remember, your PIN is your personal and private information, and you will never be asked to disclose it to a third-party.

When shopping online, always use trusted and verified websites, apps or platforms. Never be tricked or pressured into using an unsecured shopping channel.

If disposing of your personal information, then do so in a secure manner. Use a confidential waste bin for secure document destruction, tear or cut-up documents containing personal information into small pieces before disposing of them, do not dispose multiple information bearing documents at one time.

Never click on unexpected or unknown documents or web links, they can contain malware, spyware, keystroke monitoring software, or viruses, which are designed to steal your information.

Organised Crime Group's Pocket Book of Frauds

Fraud - How to Protect Your Business

Protect your Bank Accounts

Separating your personal banking and credit cards from your business accounts – this will ensure that if you are a victim the fraudsters don't get their hands on ALL your money.

Safeguard your Computer Systems

Invest in a firewall as well as anti-virus, malware, and spyware detection software.

Enhance Password Securities

Don't use personal information like family names, addresses, and phone numbers. Another step that you can take to secure your IT systems is to have a password policy. Ensure that you regularly change your passwords every 60 to 90 days.

Business Email Compromise

Be aware of emails that note a change of financial data, attachments, links, unusual content and requests. Be certain that your team is validating changes to financial data by phone with a trusted contact every time!

Workforce Education & Awareness

Employees are perhaps your biggest point of vulnerability when it comes to fraud, but they are also your first line of defence. Hold regular training sessions on basic security threats (online and offline) and prevention measures.

Fraud - How to Protect Yourself

1. Many frauds start with a phishing email. Banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.
2. Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.
3. Do not trust unknown attachments or links.
4. Make sure your computer has up-to-date anti-virus software and a firewall installed. Ensure your browser is set to the highest level of security and monitoring to prevent malware issues and computer crimes.
5. When it comes to online fraud, the phrase *'too good to be true*' is often accurate.
6. Double-check their identity.

Report scams and fraud immediately!

You could prevent another victim from getting scammed.

Private Public Partnership

- Guernsey Integrated Money Laundering and Terrorist Financing Intelligence Task Force (GIMLIT) – 'Pilot Scheme' - 14th March 2023 Four (4) main retail banks
- Changes to the Disclosure / Terrorism legislation August 2023 – permitted disclosure between FSBs
- Pilot scheme extended to International Banks [***April 2024***] – 'NEW – MOU/DPIA'
- FIU issued '*GIMLIT Briefing Paper / FAQs*'
- First Operational Working Group Meeting
- Outcomes – Outreach / Education concerning new risks / threats

Increased Threat & Risk – Money Mules / Extortion

- How many of you have young adults aged 13 – 18?
- How many of them have access to a bank account / possess a bank card or a credit card?
- How many have access to the internet, gaming sites and social media?
- Could they be at risk from Organised Crime Groups?
- What are the consequences?
- What can we do to prevent this *RISK* & *THREAT?*
- *Educate & Prevent the Risk*

What is a ‘Money Mule’?

FIU have identified Suspicious Activity Reports (SARs) linked to suspected use of ‘MONEY MULES’

- Increasing trend identified link to serious and organised crime
- Definition - someone who allows the use of their account to receive and subsequently send criminal money
- Criminals contact or recruit account holders including vulnerable persons, students, persons in financial trouble
- NCA estimates 6 in 10 money mules are under the age of 30
- Offer financial incentive (very low)
- Receive funds into bank account from 3rd parties
- Transfer similar figures to another 3rd party

Case Study – Money Mules

- Person A – Student ‘Aged 17’
- Period of bank review 1st August 2022 to 1st March 2023
- Criminality identified Fraud / Money Mule / Layering
- Total credit turnover £68,000 +
- Suspicious multiple payments from / to 3rd parties using payment service provider
- Contact customer, vague re source of funds, reluctant to provide info, further contact admitted being part of a stock scam and is being used as a money mule
- Similar Modus Operandi
  - Multiple BACs credits from UK Third Party accounts, similar area sort-codes
  - Reference ‘FX’, ‘Here you go babe’, ‘long number/P’
  - Total of £23,000+ payments in 23 online/mobile payments, payments to Revolute

Implications of Facilitating Money Laundering

- The ‘Future’ – University, High Flying Career, Travel (US/Australia)
- Conviction or suspended sentence – ML?
- Credit Rating
- No Bank Account
- No ‘Visa’ / Travel
- Potential ‘Target’ for future crime

SEXTORTION

91% of victims are young men

Some victims commit suicide

ANYONE CAN BE A VICTIM

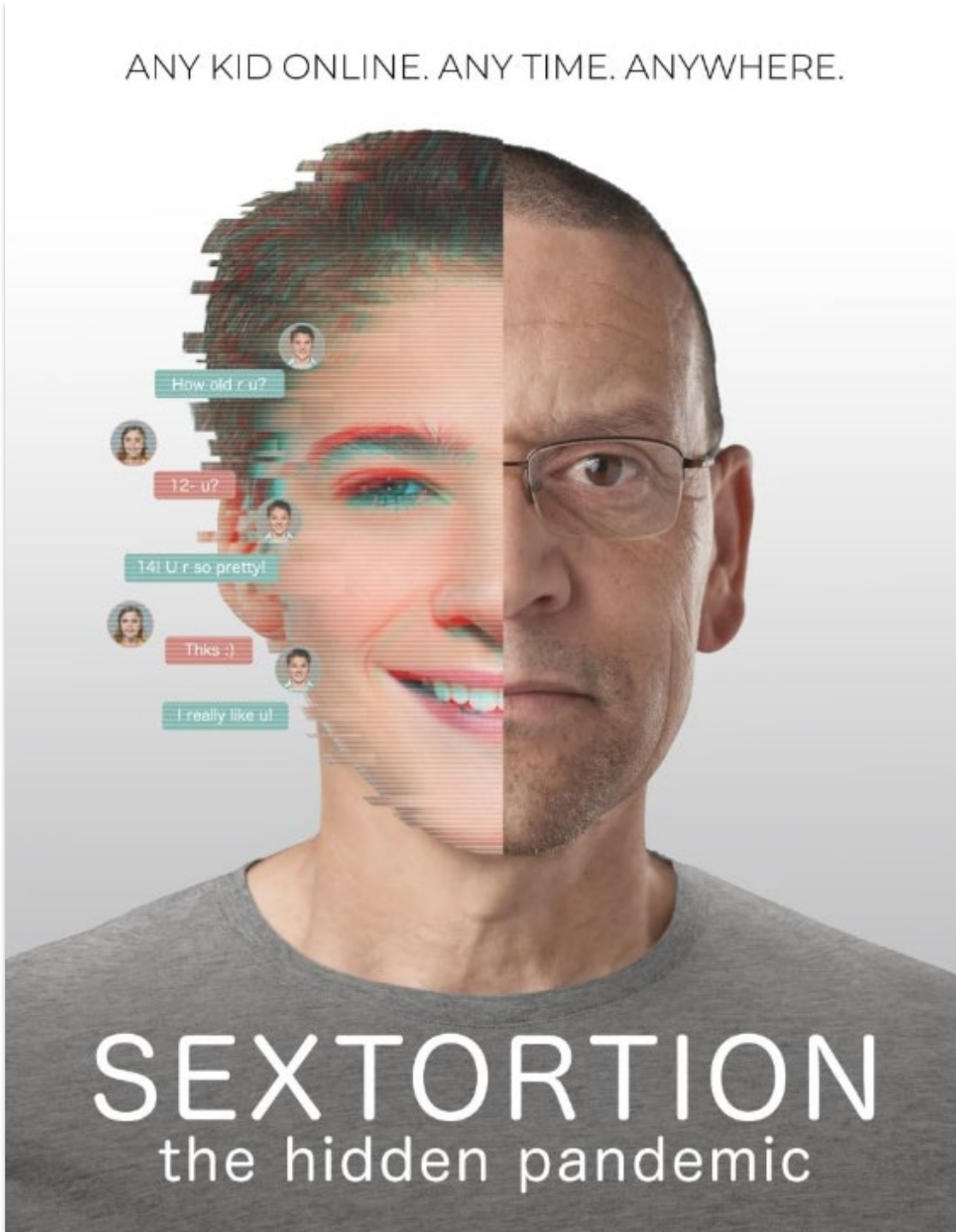
Cases have ‘doubled’ in the last year

Paying often doesn’t stop the extortion

Your computer has been ‘hacked’ not true

‘Extortion’ is an offence

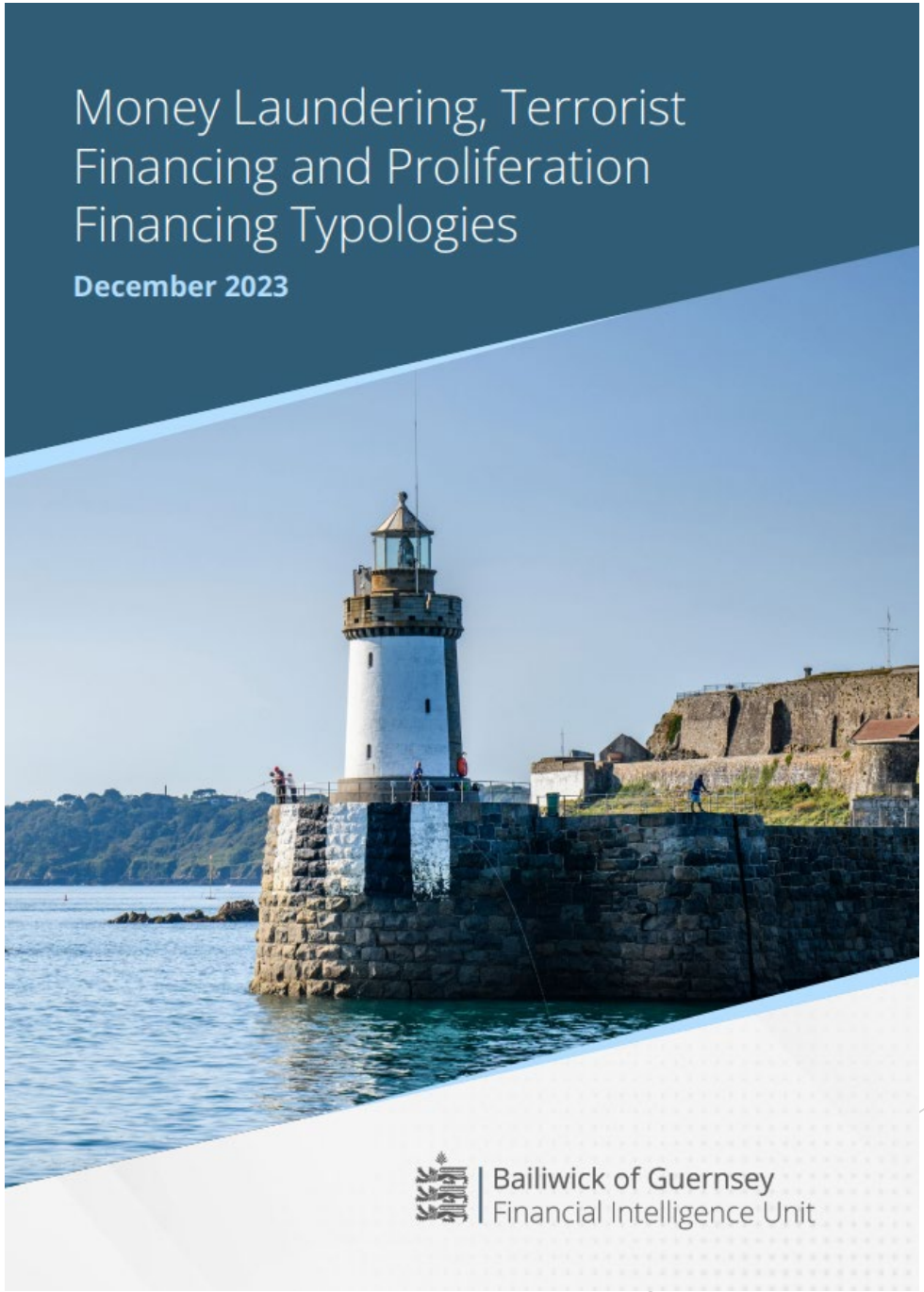
Victims tricked into sending nudes, criminals then threaten to share the pictures if money isn’t sent – Gift Cards and Vouchers



Overview

- Introduction
- Typologies
  - Fraud
  - Tax Evasion
  - Bribery & Corruption
- Sanctions Breaches
- Terrorist Financing Typologies
- Proliferation Financing Typologies
- Emerging Technology

- Other forms of Guidance
  - FIU Website



Financial Crime

Financial Sanctions

News and Resources on Financial Crime

Agencies combatting financial crime

Non-profit organisations combatting financial crime

FATF and MoneyVal

Finance industry abbreviations and terms

National risk assessment

National Strategy

Counter-Terrorism & C-T Financing Measures

MoneyVal FAQs

Share this page

Financial Crime - States of Guernsey (gov.gg)

Bailiwick of Guernsey
Financial Intelligence Unit

01481 225824
FIU@fiu.gov.gg

Search

Information | Economic Crime | Reporting | National Risk Assessment | Sanctions | Contact