SHCOG Securities Houses Compliance Officers Group

Financial Crime Update

Presented by Bruce Viney

23rd November 2023

Thank you for joining. The course will begin shortly.
To improve the experience for everyone, please:

- Mute your microphone
- Switch on your video (if comfortable to do so)

Disclaimer

This presentation, and any supporting materials, is provided for information purposes only and does not purport to constitute legal or consulting advice. Professional legal or consulting advice should be obtained before taking or refraining from any action as a result of the contents of this document.

Please note that this virtual training session is being recorded.

Challenges and Threats are Evolving Fast

The changing global threat:

- National economies and institutions are undermined by money laundering
- Fraud and cyber attacks
- The war in Ukraine and cost of living pressures
- Increasing use of criminal supply chains, networks and specialists.
- Digitalisation -> industrialising organised crime across national borders.

The new challenges of:

- Technology and social media
- Crime walking hand in hand with crime
- Professional money launderers – front men and sophisticated schemes

Getting it wrong

- Growth of international crime
- AML stops people being badly hurt
- E.g., Westpac, Deutsche Bank, Credit Suisse

The International Perspective – Organised Crime

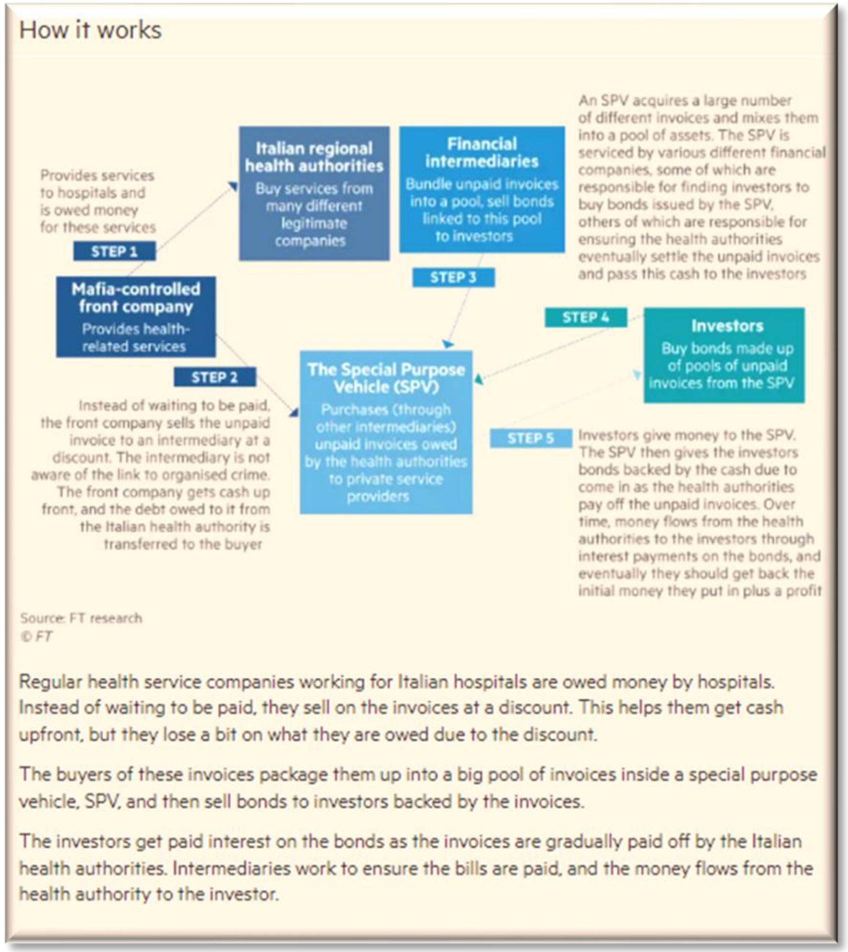
Inside the mind of a money launderer:

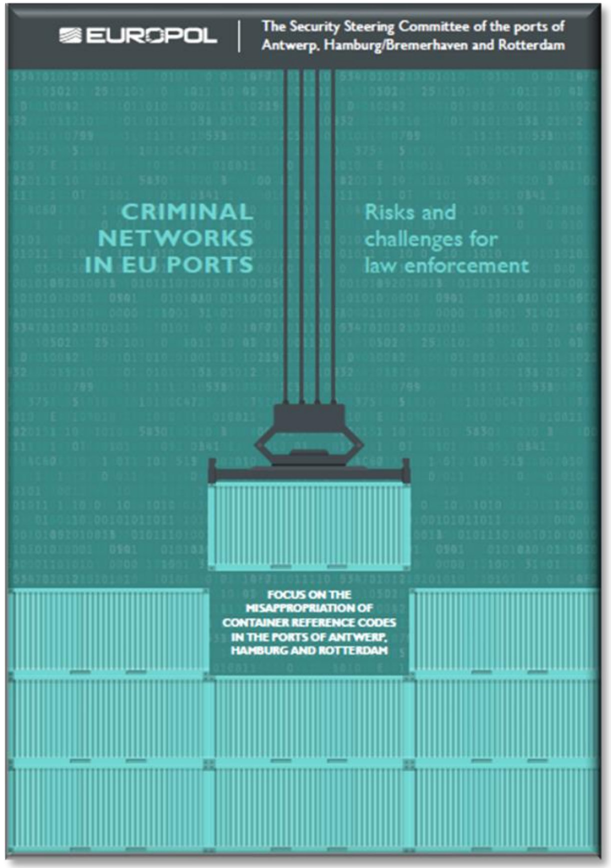
- Money Laundering, not seeking a profit
- Involved in appalling crimes:
    - Drugs
    - Trafficking
    - Slavery
    - Sexual exploitation
    - Organs and blood harvesting
    - Fraud, Cybercrimes,
    - Money laundering

Methods

- Mules and mule herding
- Kidnap and extortion
- Murder
- Exploiting the vulnerable

Infrastructural Serious Organised Crime activities





The International Perspective – Challenges and Threats

FATF:

- Real Estate
- Virtual Assets and VASPs
- Countering ransomware financing
- Updated recommendations
- Proliferation finance
- Terrorist Financing
- Beneficial ownership and transparency

Wolfsberg:

- Anti-bribery and corruption
- Financial Crime Questionnaire
- Digital customer lifecycle risk management
- Source of wealth and Source of funds
- Tax evasion
- Sanctions screening

Estimated annual income of significant terrorist groups

	Organization	Est. $m	Areas of activity	Primary sources of income
1	Taliban	2,500	Afghanistan and Pakistan	Taxes and fees, drug trafficking and mining
2	Ansar Allah (The Houthi Rebels)	2,000	Yemen	Taxes from companies and corporations, illegal oil trade
3	Hezbollah	1,200	Lebanon and Syria	Aid funds from Iran, drug trafficking
4	Al Qaeda and its affiliates	600	Global	Taxes, illegal trade (drug, arms & human trafficking)
5	Hamas	500	Gaza Strip and the West Bank	Taxes and fees, Aid funds from Iran
6	Kurdistan Workers' Party (PKK)	250	Turkey, Iraq and Syria	Illegal trade (drug, arms & human trafficking)
7	ISIS and its affiliates	150	Global	Taxes, kidnapping and ransom illegal trade (oil & Antiquities trafficking)
8	Real IRA	70	UK and Ireland	Illegal tobacco trade
9	Kata'ib Hizballah	50	Iraq and Syria	Aid funds from Iran
10	Palestinian Islamic Jihad	35	Gaza Strip and the West Bank	Aid funds from Iran

Source: Forbes Jan 2022

Terrorist Financing – Four Stages

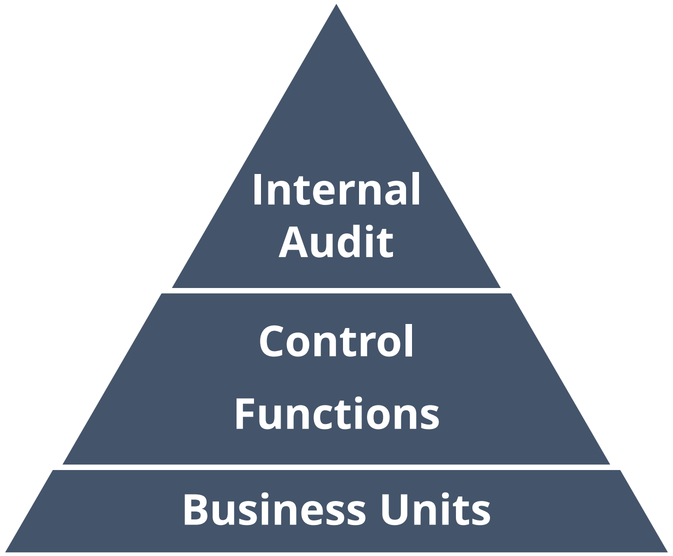
1. Collecting	2. Storing:	3. Moving (highest risk)	4. Using
• Direct donations by individuals and organisations • Use of charities and other NPOs • Criminal activities and • Legitimate businesses	• Bank accounts • Pre-paid cards • High value commodities • Used vehicles • Cryptocurrencies • Cash	• Banking and the financial sector • Money service businesses • Hawala and other informal transfer systems • Smuggling: cash, gold, gems • Cryptocurrencies – wallet to wallet	• Weapons • Materials • Equipment • Training • Media and messaging • Travel and accommodation

Key determinants: Volume; Risk; Convenience; Simplicity; Costs and Speed

Challenges and Trends – What Are We Getting Wrong?

Frequent breaches identified by the FCA include:

- Inadequate customer due diligence (CDD) procedures
- Inadequate enhanced due diligence (EDD), specifically in relation to Politically Exposed Persons (PEPs)
- Inadequate client risk assessments
- Inadequate firm-wide risk assessments
- Inadequate training of staff responsible for AML supervision
- Inadequate documentation of risk-assessments and measures taken to monitor risk'



Source: HM Treasury, Anti-Money Laundering and countering the financing of terrorism: Supervision Report 2020 - 22

Economic Crime and Corporate Transparency Bill

- Making it easier to prosecute companies for ‘economic crimes’
- an organisation will be criminally liable when part or all of a specified economic crime is committed in the UK by a senior manager of that company or partnership.
- Who is a ‘senior manager’?
- What are ‘economic crimes.

Economic Crime and Corporate Transparency Act

- Introduces a Corporate Failure to Prevent Fraud offence, where a specific fraud offence is committed by an employee or agent, for the organisations benefit.
- This is regardless as to whether the senior management were aware of the fraud.
- This will apply only to large corporate bodies and partnerships across all sectors
- Penalty will be an unlimited fine
- Government will provide guidance

Defence:

- Organisations will be able to avoid prosecution if they have reasonable procedures in place to prevent fraud

The Farage(go) of PEPs

- The issues surrounding de-risking and inclusive finance
- FCA Review issued 5 September 2023 - Not a change of regulation or laws:
    - Application of the definition of PEPs to individuals
    - Conducting proportionate risk assessments of UK PEPs and RCAs
    - Applying EDD and ongoing monitoring proportionately and in line with risk
    - Deciding to reject or close accounts for PEPs and RCAs
    - Effectively communicating with their PEP customers
    - Keeping their PEP controls under review to ensure they remain appropriate.
- Review ends 24/06/24

FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes

July 2017

The Farage(go) of PEPs

- *The FCA expects that a firm will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or of a family member or known close associate of a PEP). A firm may, after collecting appropriate information11 and completing its assessment, 12, conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases will it be appropriate to decline or close that relationship*
- *FG 17/6 2.13*

- *If, having assessed the risk associated with the customer and decided on an appropriate level of enhanced due diligence measures in line with this guidance, a firm is unable to apply those measures, a firm needs to comply with the requirement13 not to establish, or to terminate, a business relationship*
- *FG 17/6 2.14*

Proliferation Financing

Risk assessment by relevant persons in relation to proliferation financing

1. A relevant person must take appropriate steps to identify and assess the risks of proliferation financing to which its business is subject.
2. In carrying out the risk assessment required under paragraph (1), a relevant person must take into account
   a. information in the report referred to in regulation 16A (risk assessment by the Treasury); and
   b. risk factors including factors relating to:
   i. its customers;
   ii. the countries or geographic areas in which it operates;
   iii. its products or services;
   iv. its transactions; and
   v. its delivery channel

Proliferation – a rising danger to world peace

- “Now that the US, steeped in the Cold War mentality, has gone to extremes in its anti-DPRK military provocations, it is very important for the DPRK to accelerate the modernisation of nuclear weapons in order to hold the definite edge of strategic deterrence,” Kim Jong-un The Times, 28 September 2023

- Kim spoke of “the need to push ahead with the work for exponentially boosting the production of nuclear weapons and diversifying the nuclear strike means”,

Key Actors in PF – UK National Risk Assessment

*"The PF threats that the UK is most likely to be exposed to relate to the UK's central role as a global **provider of financial and corporate services** in support of the legitimate trade in **sensitive items**, even items that are not procured from the UK, as well as the ability for actors to establish **shell companies** in the UK to conceal a wider network of PF-related activity.*

*To a lesser extent, the UK may also face PF threats as **a jurisdiction where proliferators can raise revenue and procure proliferation sensitive and other dual-use items**"*

*"The UK has a robust, bespoke regulatory framework in place to combat the threat posed by PF. A key focus is the implementation of UK and UN sanctions regimes on **DPRK, Iran and chemical weapons** activity"*

Challenges and Emerging Threats

- Increasingly PF actors are focusing on purchase and sale of elementary and replaceable components.
- Identification of both DUG and PF sensitive items requires specialist knowledge.
- PF networks are often complex:
  - Front companies
  - Agents
  - False or obscure end-users and/or end use
- Fragmented nature of trades, multiple parties, sanctions evasion
- Cryptocurrencies and block chain technology (DPRK known to use crypto for fundraising, stockpiling and circumvention).
- Advanced manufacturing techniques (3D printing, synthetic biology, chemical synthesis, nano-biotechnology etc.)

Proliferation Financing – Indicative risks

- Involvement of individuals or entities in foreign country of proliferation concern
- Involvement of individuals or entities in foreign country of diversion concern
- Individuals or entities involved or their details (such as addresses or telephone numbers), are similar to, or may be connected to, parties listed at the time under WMD-related sanctions or export-control regimes, or they have a history of involvement in export control contraventions
- Presence of items controlled under WMD export control regimes or national control regimes
- Activity that does not match customers’ or counterparties business profiles, or end-user information does not match end-user’s business profile

Key Actors in PF – UK National Risk Assessment - DPRK

- The UK has in place an autonomous DPRK sanctions regime
- The purposes of the regime are to restrict the ability of North Korea to carry on banned programmes and to promote the abandonment of these, as well as the decommissioning of the DPRK's banned weapons, and otherwise promote peace, security and stability on the Korean peninsula
- 2006: Prohibitions intended to restrict DPRK CBRN* capability and reversing its CBRN programmes.
- 2009: Expansion of the arms embargo.
- 2013:Further restrictions on development of technology in relation to the CBRN capabilities; added luxury goods to list of banned imports.
- 2016: Further expansion of measures
- 2017 included financial restrictions, restrictions on the import of energy resources, and required countries to expel North Korean workers.

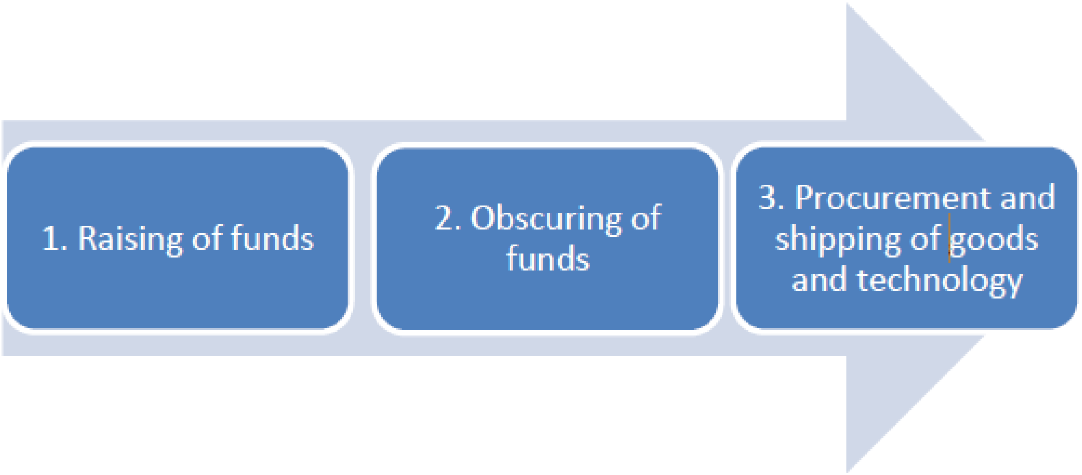
*Chemical, Biological, Radiological, Nuclear;

Key Actors in PF – UK National Risk Assessment - Iran

- The UK implements two autonomous sanctions regimes that target specific activities carried out by actors in Iran:
  - The Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019 which is intended to:
    - ensure UK compliance with UNSCR 2231;
    - promote the abandonment by Iran of nuclear weapons programmes;
    - restrict the ability of Iran to develop nuclear weapons and nuclear weapons delivery systems; and
    - promote implementation of the Joint Comprehensive Plan of Action
- The Iran (Sanctions) (Human Rights) (EU Exit) Regulations 2019. The Regulations impose sanctions measures on Iranian individuals and entities involved in this activity.

The stages of proliferation finance

- **Fundraising**: the proliferator sources funds from state budgets, or from illegitimate or legitimate commercial or criminal activities conducted overseas by or on behalf of state actors.
- **Disguising and placing funds** into the financial system: proliferators rely on a network of businesses, front companies, opaque ownership structures and brokers to ensure that everything appears geographically separate from sanctioned countries.
- **Procuring materials** and technology using those funds: the proliferator accesses the international financial system to pay for goods, materials, technology and logistics needed for its WMD programme.



Proliferation Financing – Indicative risks

- End-user is not identified
- Involvement of an individual connected with a country of proliferation concern
- An order for goods is placed by firms or individuals from foreign countries other than the country of the stated or suspected end-user
- Use of cash in transactions for industrial items
- Involvement of front companies, also shell companies
- Customer is a manufacturer/dealer in products which are subject to export controls
- Pattern of transactions of a customer or counterparty, declared to be a commercial business, suggest they are acting as a money-remittance business
- Customers involved, directly or indirectly, with Dual Use Goods

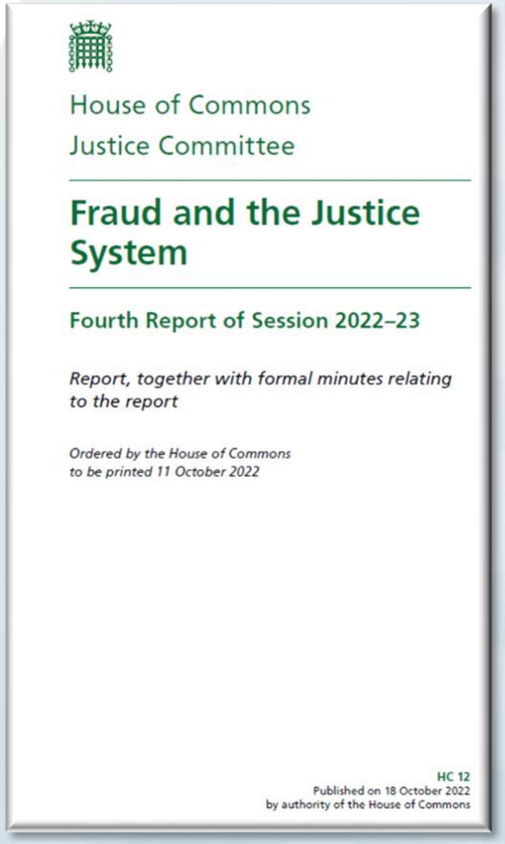
Sanctions – Getting it right

FCA released September 2023: Key findings from FCA assessments of sanctions systems and controls in financial services firms.

1. **Governance and oversight:** The ability to monitor and review the effectiveness of sanctions implementation through management information (MI) is important, as is ensuring that sanctions reporting is calibrated to the UK regime.
2. **Skills and resources:** Sanctions teams need to be properly resourced to avoid backlogs in dealing with sanctions alerts and enable a quick reaction to sanctions risks.
3. **Screening capabilities:** Sanctions screening tools need to be adequately calibrated and include the necessary requirements under the UK regime.
4. **Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures:** Effective CDD and KYC are a cornerstone of effective compliance with sanctions requirements.
5. **Reporting breaches to the FCA:** We expect firms to make timely and accurate reporting to us on potential sanctions breaches.

Fraud – How worried should we be?

- *‘There is currently an epidemic of fraud in England and Wales. The level of fraud has been increasing year on year and this growth accelerated during the pandemic to an unprecedented level’*
- 3.8 million fraud offences in UK up to June 2022 – ONS


House of Commons
Justice Committee

Fraud and the Justice System

Fourth Report of Session 2022–23

Report, together with formal minutes relating to the report

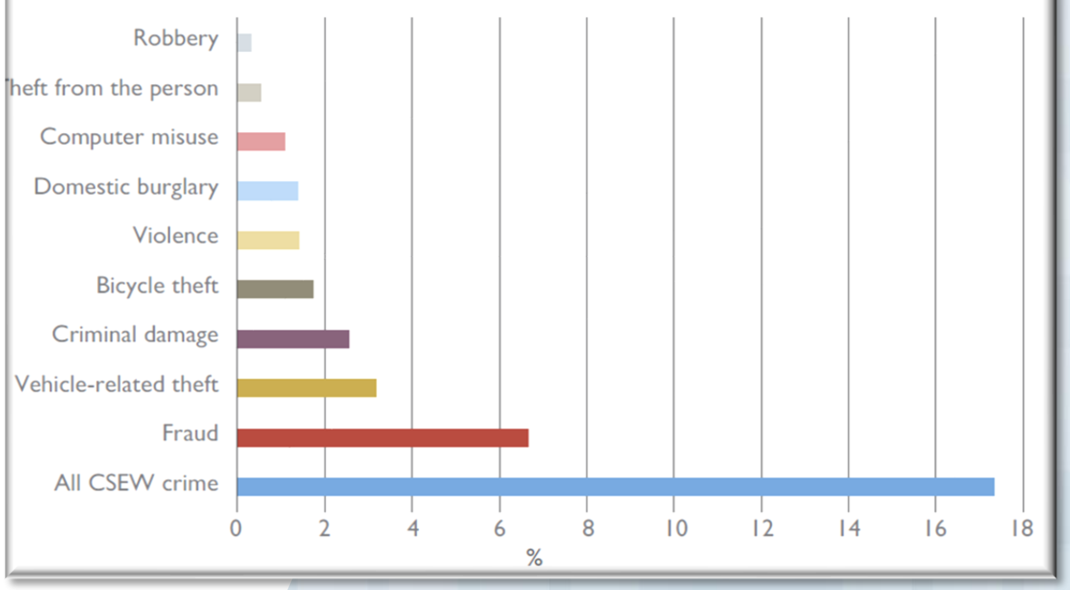
Ordered by the House of Commons to be printed 11 October 2022

HC 12
Published on 18 October 2022
by authority of the House of Commons

Introduction to Fraud

- Fraud is the most commonly experienced crime in England and Wales today.
- It accounts for approximately 41% of all crime against individuals.
- A person aged 16 or over is more likely to become a victim of fraud than any other individual type of crime, including violence or burglary.
- It costs the economy billions every year.
- Most fraud is now happening online and often involves social engineering of the victim

Figure 3: The likelihood of being a victim of different crime types



Cyber Fraud

- More than 80% of UK organizations experienced a successful attack in 2021/2022
- Over a 12-month period, ransomware attacks affected 73% of UK organizations
- 43% of ransomware attacks in the UK were stopped prior to data encryption
- 13% of UK organizations ended up paying the ransom
- The average cost of ransomware attacks in the UK was around $1.08 million
- 77% of UK organizations have cyber security insurance

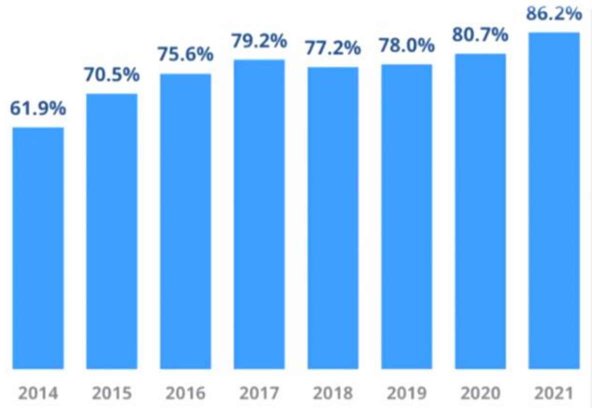


Figure 2: Percentage of organizations compromised by at least one successful attack.

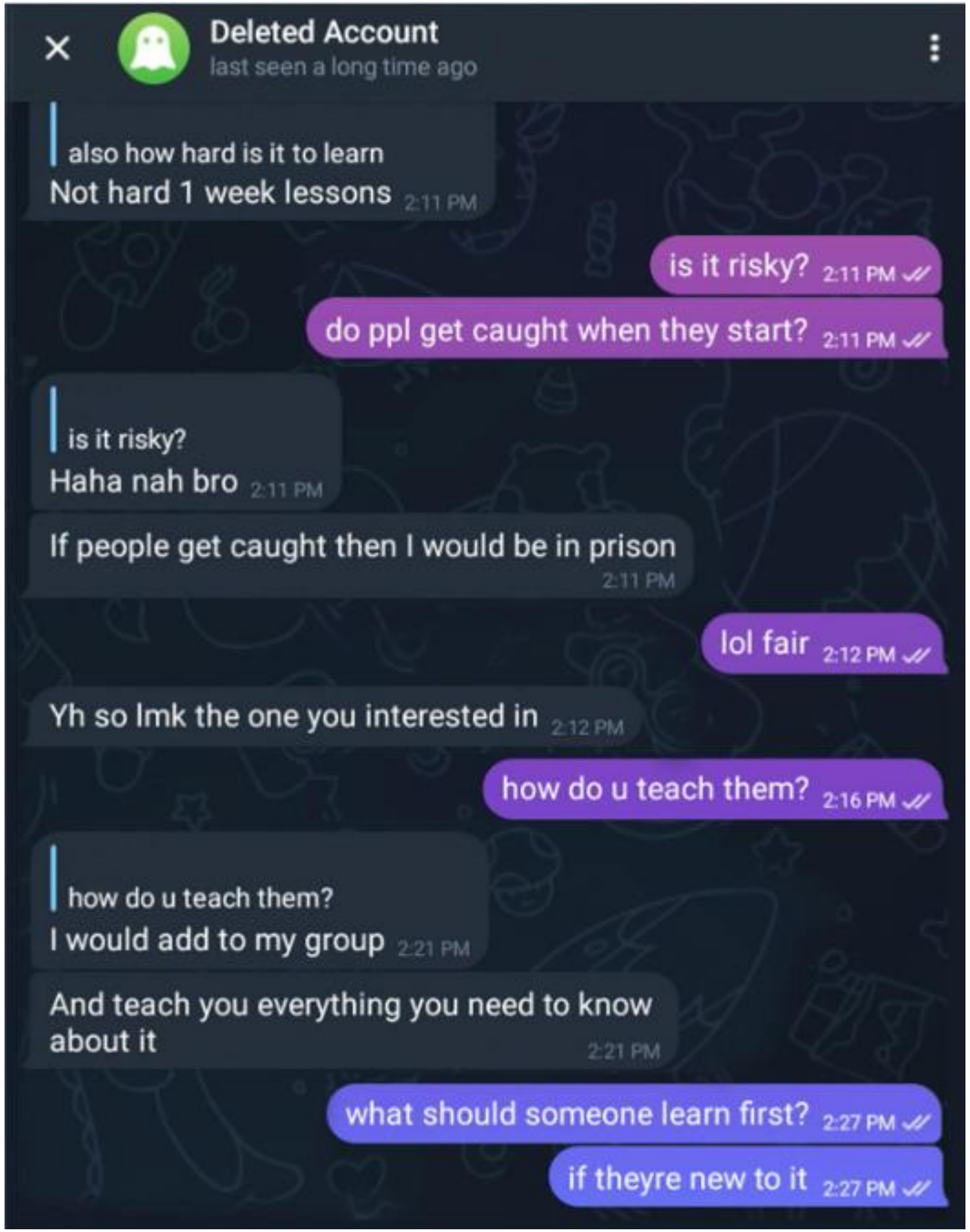
CyberEdge Group 2021 Cyberthreat Defense Report

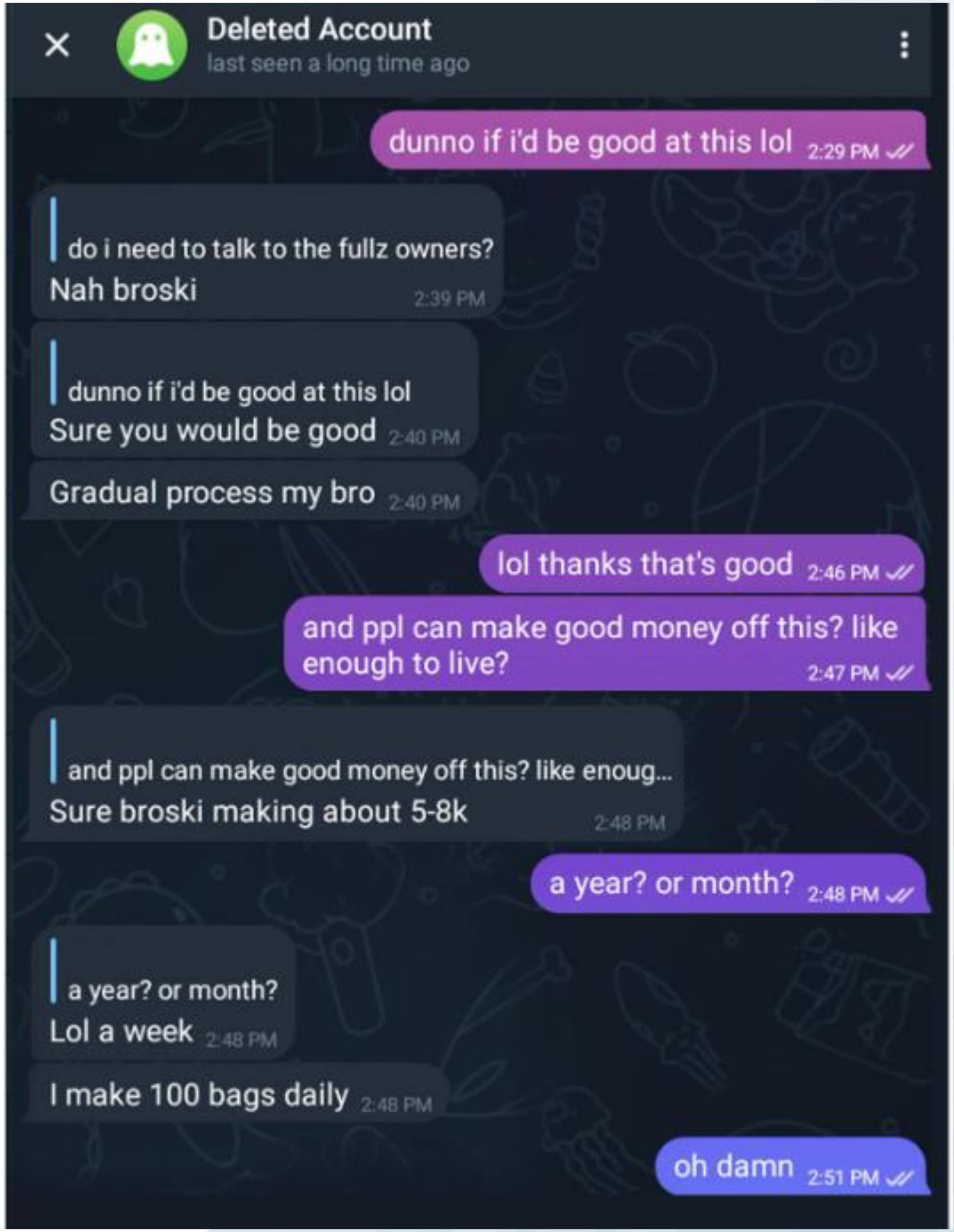
Source: Comparitech

Common Phishing Attacks

- Phishing attacks up by 61% in 2022
- Equates to 255 million detected phishing attacks
- 76% Of these relate to credential harvesting
- 48% rise in Zero hour (never before) threats
- Rise in multichannel threats

- Standard phishing emails
- Spear phishing
- Whale or CEO phishing
- Phishing to plant malware
- Vishing
- SMiShing
- Crypto asset frauds
- Business email compromise attacks
- And many others…


Deleted Account
last seen a long time ago
also how hard is it to learn
Not hard 1 week lessons 2:11 PM
is it risky? 2:11 PM
do ppl get caught when they start? 2:11 PM
is it risky?
Haha nah bro 2:11 PM
If people get caught then I would be in prison 2:11 PM
lol fair 2:12 PM
Yh so lmk the one you interested in 2:12 PM
how do u teach them? 2:16 PM
how do u teach them?
I would add to my group 2:21 PM
And teach you everything you need to know about it 2:21 PM
what should someone learn first? 2:27 PM
if theyre new to it 2:27 PM


Deleted Account
last seen a long time ago
dunno if i'd be good at this lol 2:29 PM
do i need to talk to the fullz owners?
Nah broski 2:39 PM
dunno if i'd be good at this lol
Sure you would be good 2:40 PM
Gradual process my bro 2:40 PM
lol thanks that's good 2:46 PM
and ppl can make good money off this? like enough to live? 2:47 PM
and ppl can make good money off this? like enoug...
Sure broski making about 5-8k 2:48 PM
a year? or month? 2:48 PM
a year? or month?
Lol a week 2:48 PM
I make 100 bags daily 2:48 PM
oh damn 2:51 PM

How is your firm doing?

- ✓ Does your business risk assessment follow a well-considered, fully documented and consistently applied methodology that is appropriate for the type, nature and scale of your firm's business?
- ✓ Is your business risk assessment up to date? Consider the rapidly changing nature of the business world, regulation and your own business.
- ✓ Do your AML policies and procedures reflect what is in your business risk assessment?
- ✓ Do your three lines of defence thoroughly understand their role in AML compliance, and can you evidence that?
- ✓ Can senior management identify the key money laundering and terrorist financing risks of their firm. Do senior management receive the right information on the operation and monitoring of these controls, and do they challenge what they are told? Are those challenges documented?
- ✓ Are customer risk assessments carried out in line with the outcomes and requirements of the business risk assessment?

How is your firm doing?

- ✓ Do your staff understand that risk is on a continuum, even though your firm might use the categories of low, medium and high risk?
- ✓ Do your staff understand the relative risks that may attach to customers ranked as high risk? For example, the fact that PEPs, which are always treated as high risk in the UK, in fact may have very different levels of risk within that high risk ranking?
- ✓ Do your staff ensure that the full business of a corporate customer is fully understood and recorded?
- ✓ Are your staff able to articulate their responsibilities in terms of reporting suspicions? Do they know what a suspicion is defined as and to whom they should report?
- ✓ Do your staff receive regular, role-focused training, which is practical, engaging and based on real life experiences?

Thank You