NATIONAL TRADING STANDARDS
Scams Team

Bored of fraud? It's time for a change.

National Trading Standards Scams Team Online Conference

27th March 2025

Welcome

- Who we are
- The theme of today's conference
- Housekeeping
- Speakers and presenters

NATIONAL TRADING STANDARDS
Scams Team



The Lord Michael Bichard KCB

Team update and STRICT:
Louise Baxter MBE, NTS Scams Team.

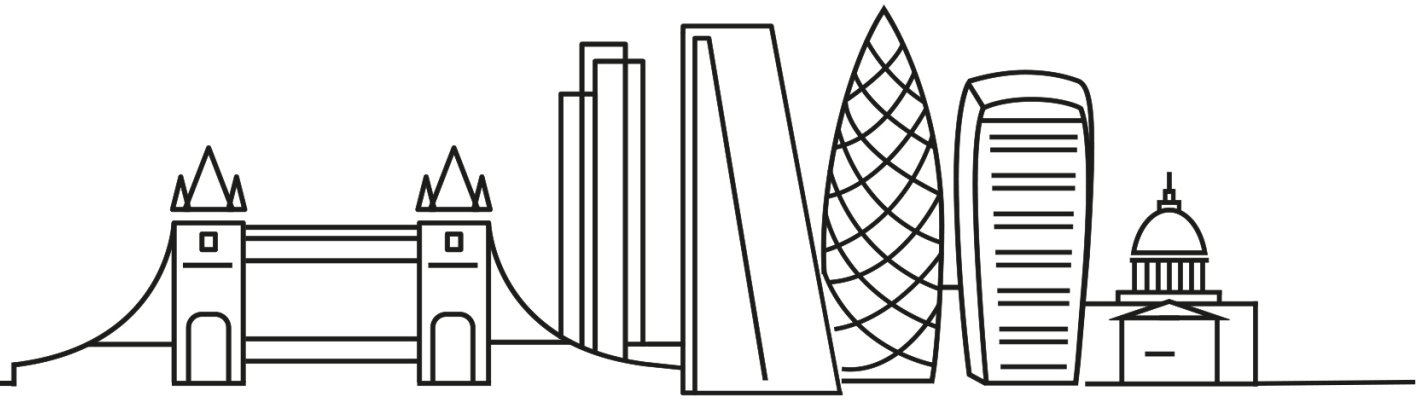
Keynote speakers:
Nik Adams, Deputy City of London Commissioner and Nick Sharp, Deputy Director for Fraud, National Economic Crime Centre.

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

Countering the fraud threat: A law enforcement response

Deputy Commissioner Nik Adams – City of London Police
Deputy Director Nick Sharp – National Economic Crime Centre



City of London Police responsibilities:

Setting the national fraud, economic and cyber crime policing strategy and leading and coordinating the police response to fraud & cyber

Co-ordinating national fraud reporting of 1.2M reports and 750,000 calls each year through Action Fraud, national triaging and allocation of fraud cases and intelligence. Over 500,000 victims support & 88,784 cases disseminated for investigation.

Investigation of nationally significant, serious and complex fraud
Last year, 300+ arrests, 200+ charges & almost 600 OCG disruptions.
Leadership and coordination of victim care.

Workforce development, including training, continuous professional development and dissemination of good practice across police forces.
1520 courses delivered nationally.

Collation, interpretation and reporting of national fraud policing performance



The 4 P approach provides a framework for the sophisticated response that is required to tackle the nature of fraud, economic and cyber crime

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

Scale of the threat

Fraud remains the single biggest crime type in the UK.

Fraud makes up 39% of all crime, rising to 50% with cybercrime

NECC
NATIONAL ECONOMIC CRIME CENTRE

90 % of fraud has online element with growing prevalence of AI

International Collaboration



67% of fraud is cyber enabled



1 in 18 people

Have been a victim of fraud

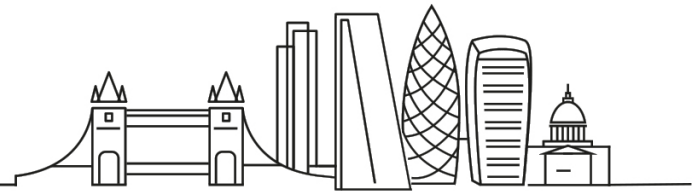
3.8m fraud incidents

YE September 24

£166.1 Billion losses annually



70% of Fraud has international element

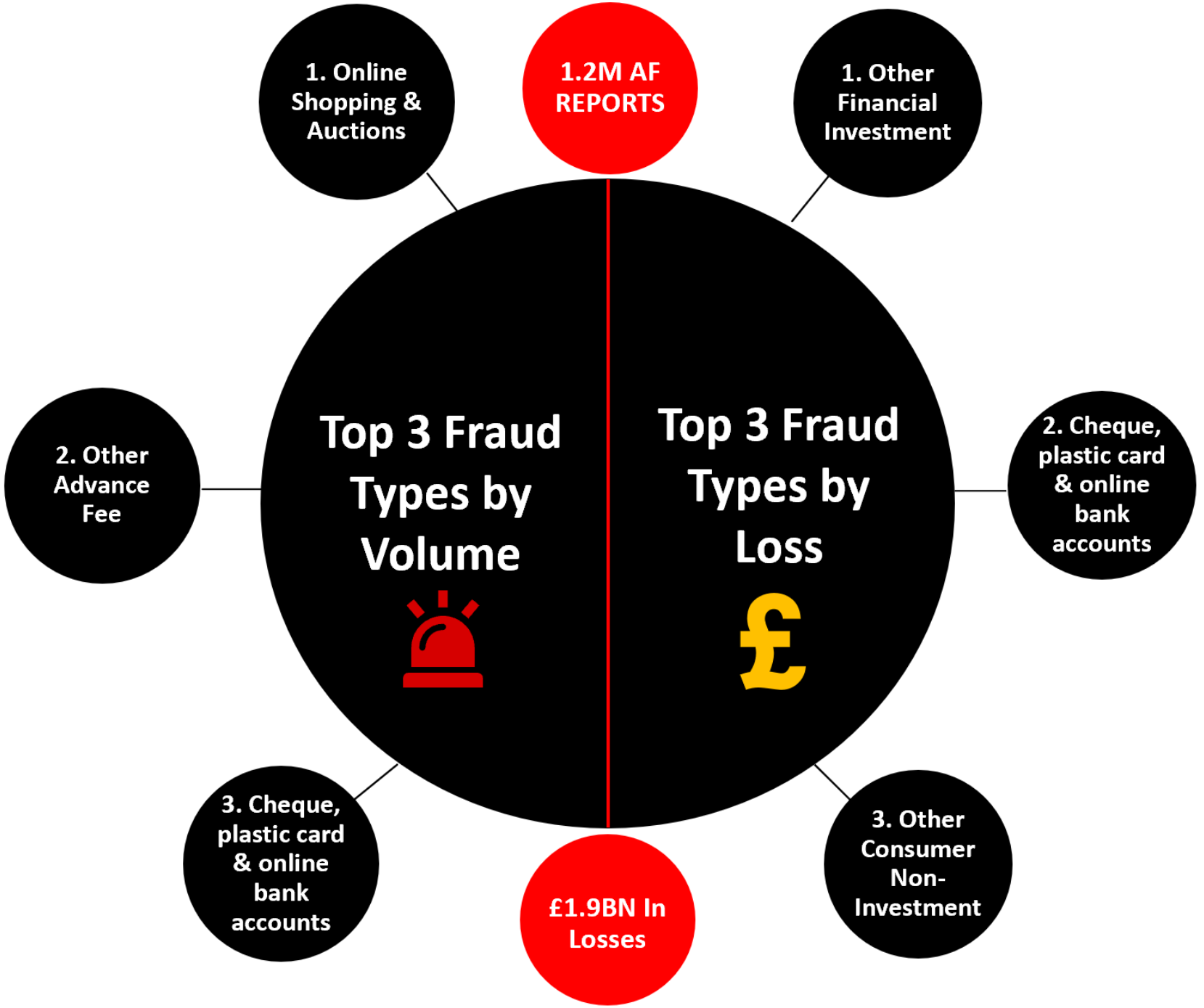


CITY OF LONDON POLICE

A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

Nature of fraud

Policing activity is prioritised against the highest harm offenders, and we target support to the most vulnerable victims

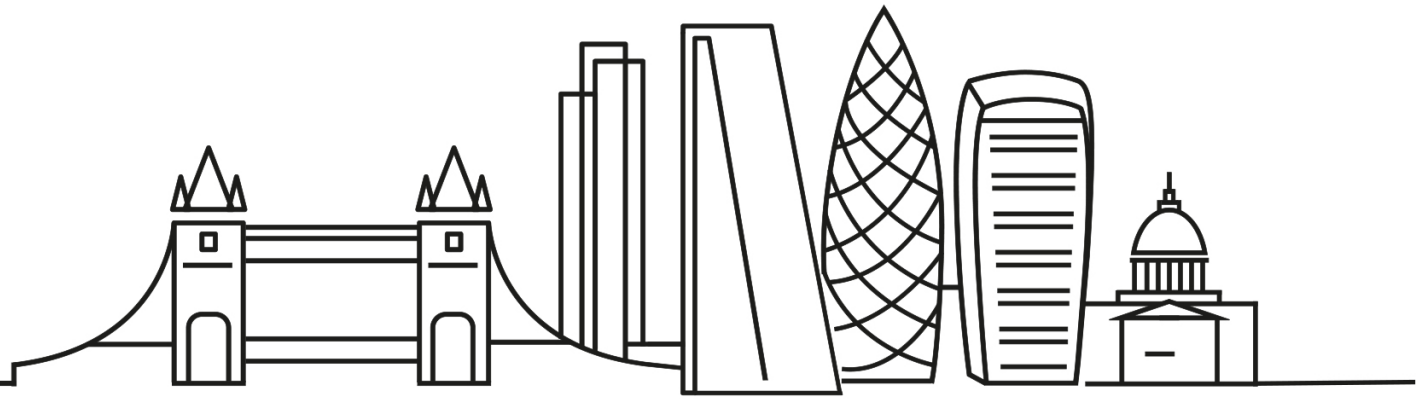


CITY OF LONDON POLICE

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

Fraud and Cyber Crime Reporting and Analysis Service



A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

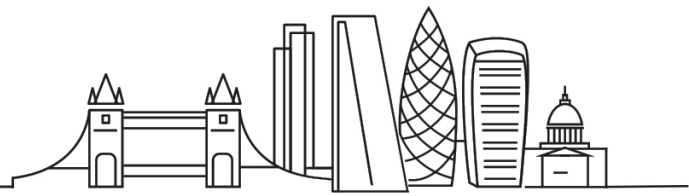
Fraud and Cyber Crime Reporting and Analysis Service

What the new service aims to do:

- Improving the **speed and quality of information** provided to law enforcement & stakeholders.
- **Easier reporting** of fraud and cyber crime for everyone.
- **Victim updates** so people know what's happening.
- **Targeted timely advice** on how to avoid the latest threats.
- **Block and disrupt** crime through providing real time information to institutions and organisations who can take down the fraudulent sites, activity and bank account we know are enabling criminal activity.

CITY OF LONDON POLICE

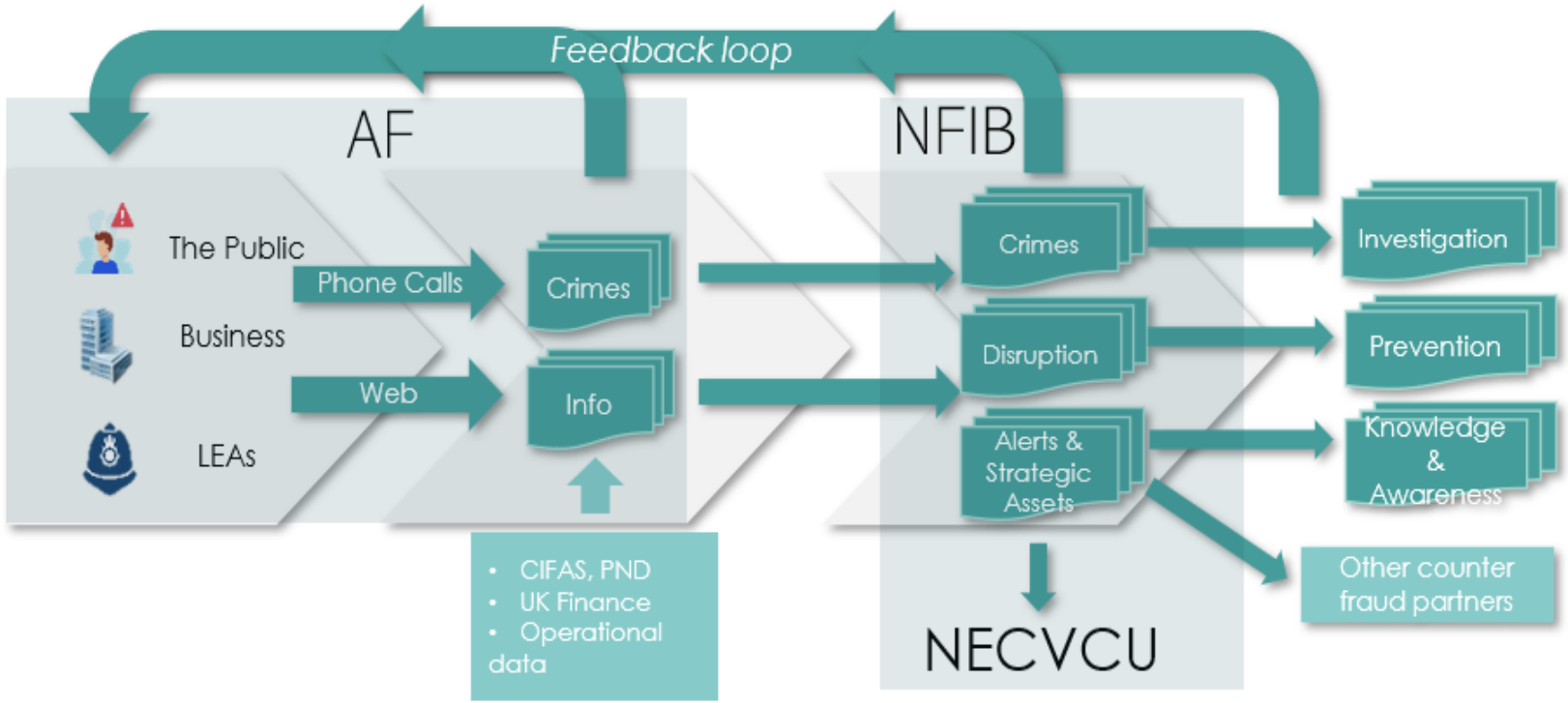
NECC
NATIONAL ECONOMIC CRIME CENTRE



NECC
NATIONAL ECONOMIC CRIME CENTRE

The Journey of Fraud Report

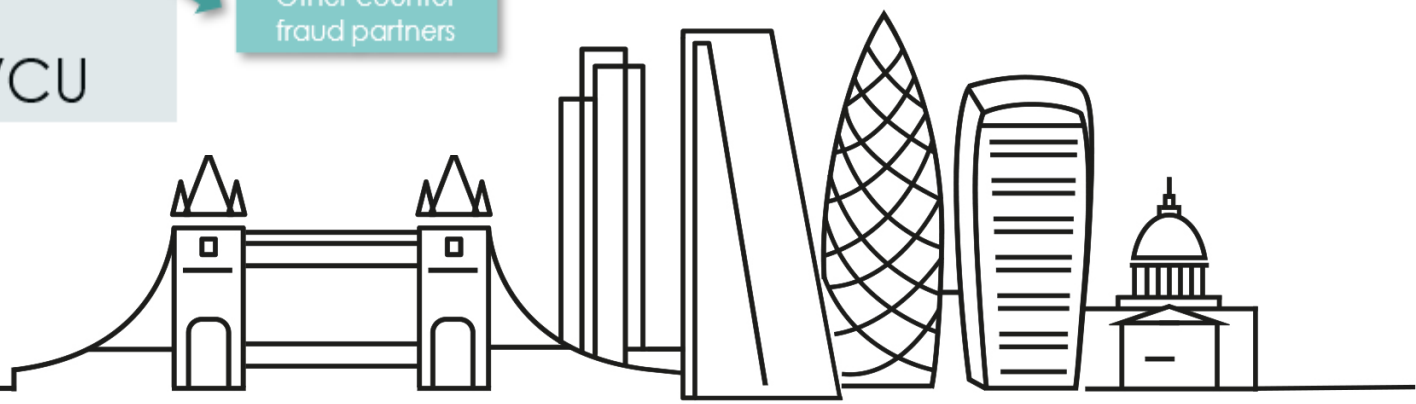
CITY OF LONDON POLICE



• Action Fraud is the national reporting service for fraud and cyber crime (website and contact centre)

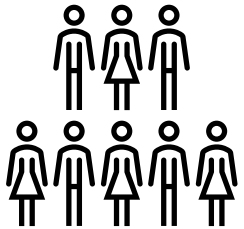
• NFIB analyses and disseminates crime packages, intelligence products and PROTECT information to UK policing, LEAs and private sector partners

• NECVCU provides bespoke support to vulnerable victims, and oversees the national delivery of PROTECT advice to non-vulnerable victims



A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

National Economic Crime Victim Care Unit



555,481
Total victims supported OCT 24

1

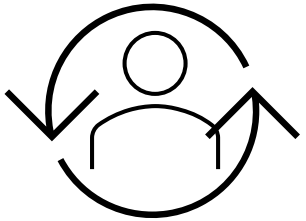
477,329
Victims Engaged at Level 1

2

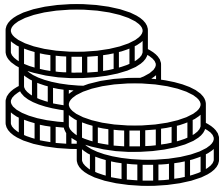
78,512
Victims Engaged at Level 2

3

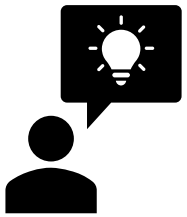
1514
Victims Escalated to Level 3



391
Repeat Victims

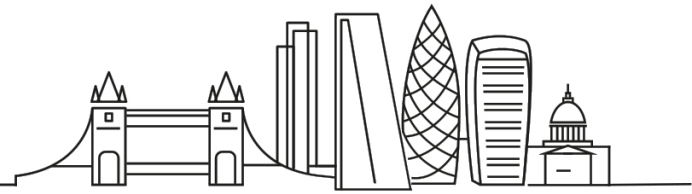


£4,929,361.13
Recovered by Victims Following NECVCU Support



567
Service Reusers

CITY OF LONDON POLICE

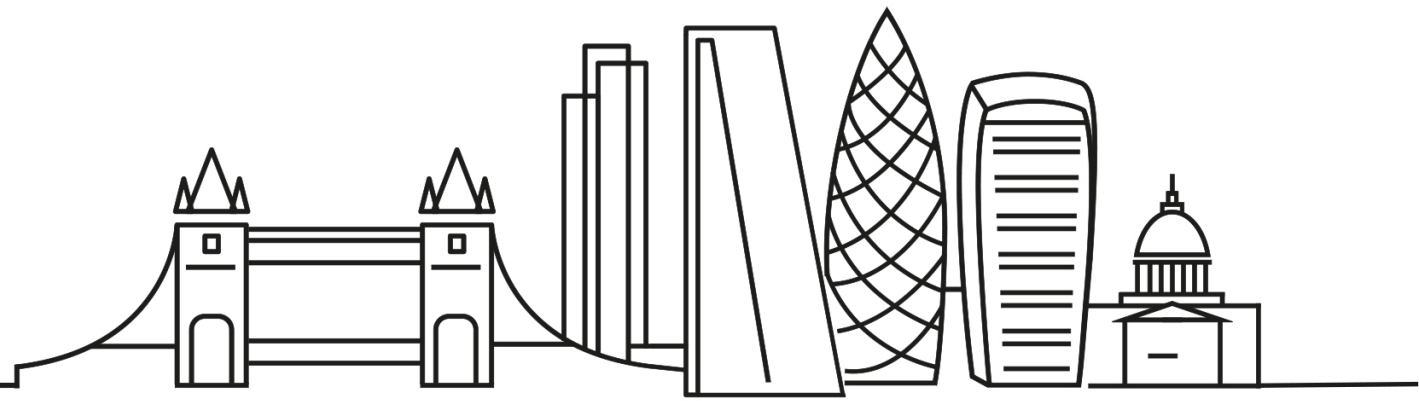


A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

Pursuing the Criminals

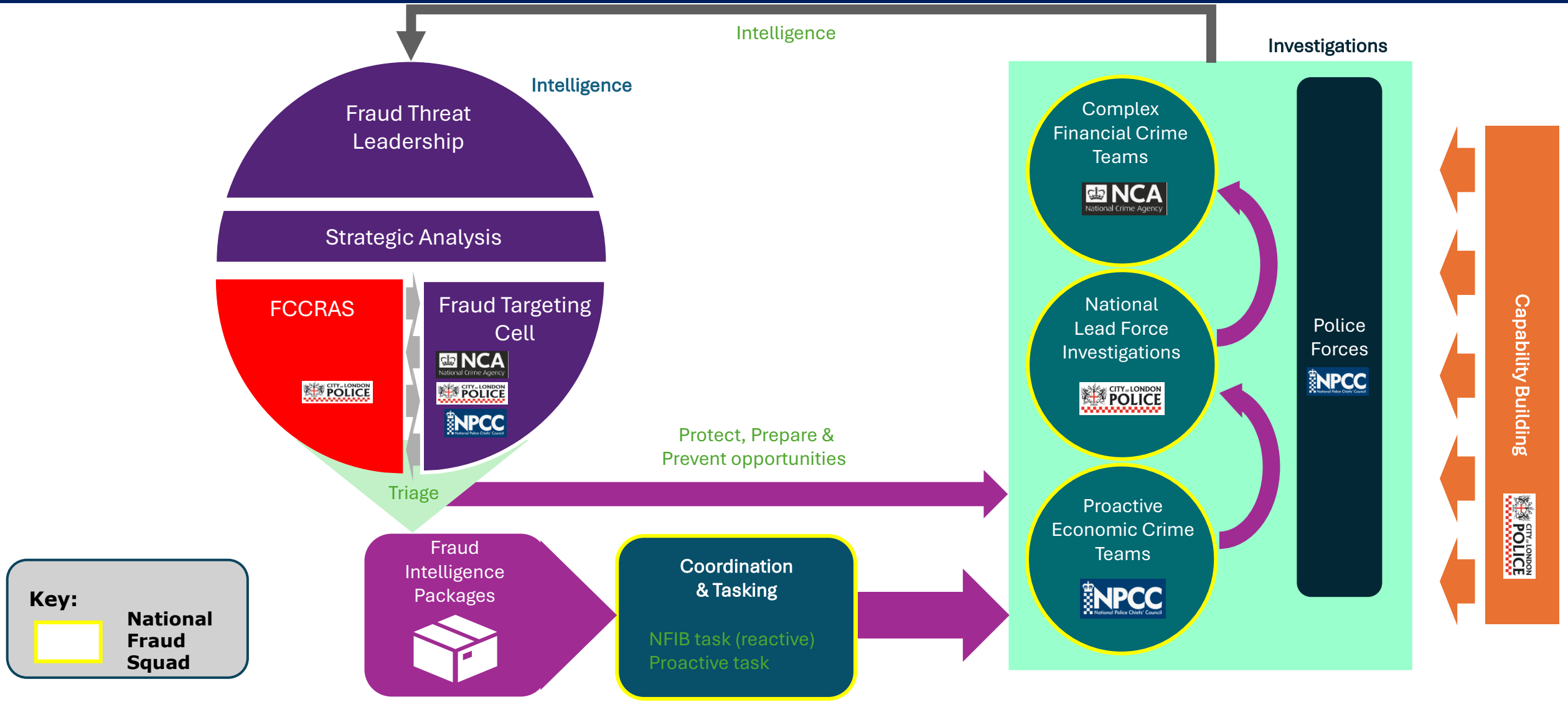


A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

The National Fraud Network



Proactive Investigations

National tasking and co-ordination of **proactive fraud investigations.**

- **Op Duper 2**: 100 referrals by forces. 100 victims given trueblocker

- **Op Stargrew:** 480,000 credit card stolen. 63% increase is NFIB disseminations due to Stargrew.





Intelligence Development Team proactively targeting high harm fraud offenders

- **Op Henhouse 4**: 422 Arrests, £7.5m seized
- **Emma 10**: 76 arrests, 43 search warrants, £818,000 cash & crypto seized.

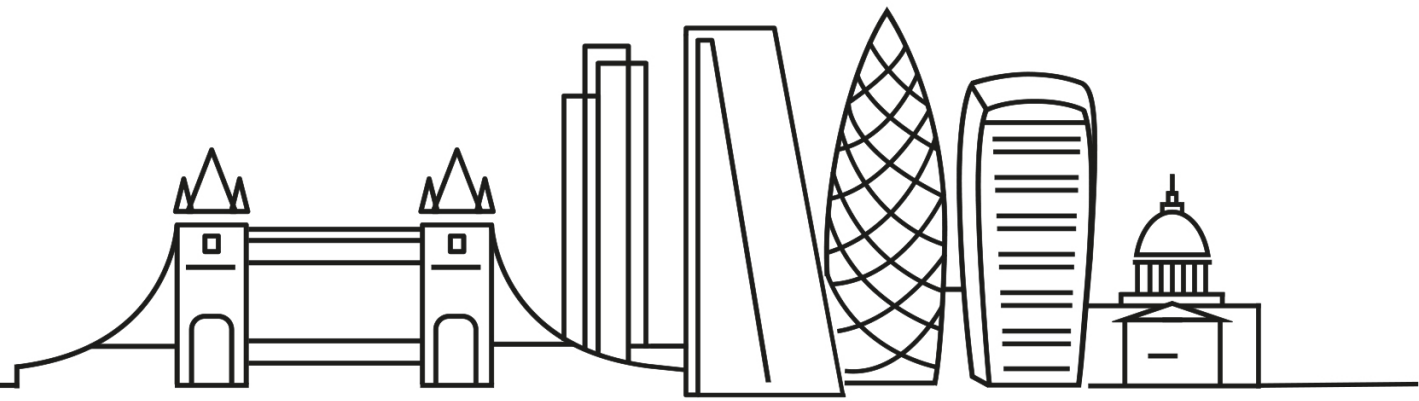
Op Neogamy: NFIB checked over 100,000 entities linked to "Russian Coms" platform.


NECC
NATIONAL ECONOMIC CRIME CENTRE
CITY OF LONDON POLICE
K80179
TARIAN
2025/02/18 04:56:22

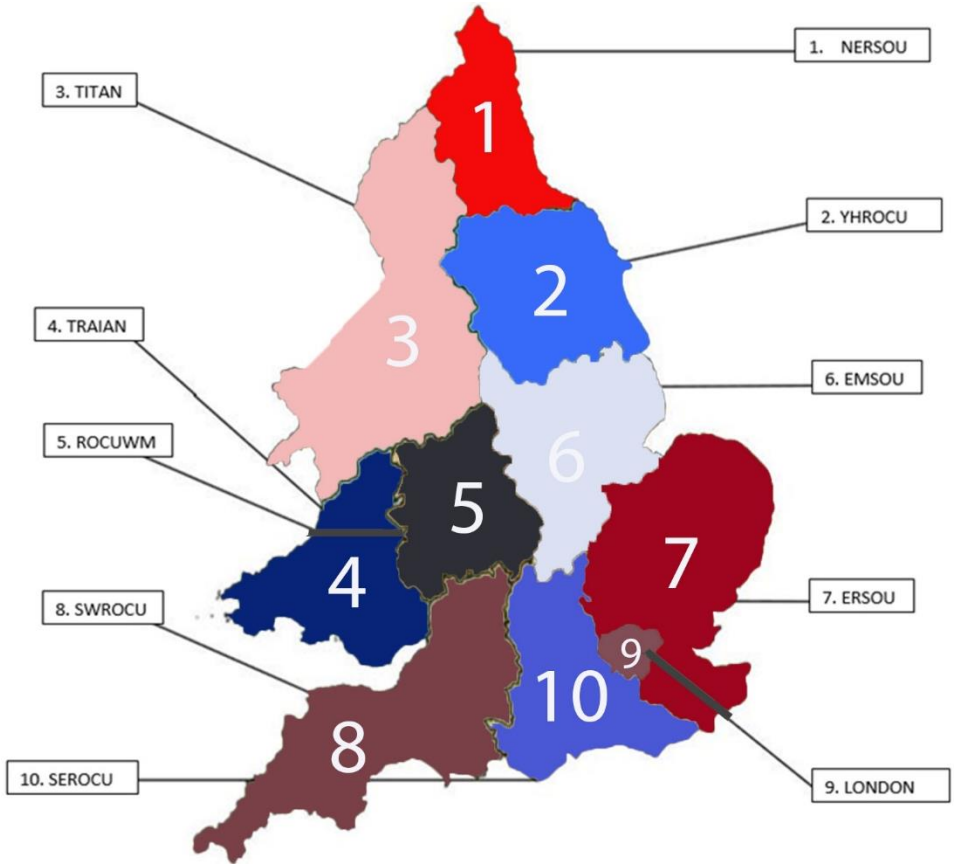
NECC
NATIONAL ECONOMIC CRIME CENTRE

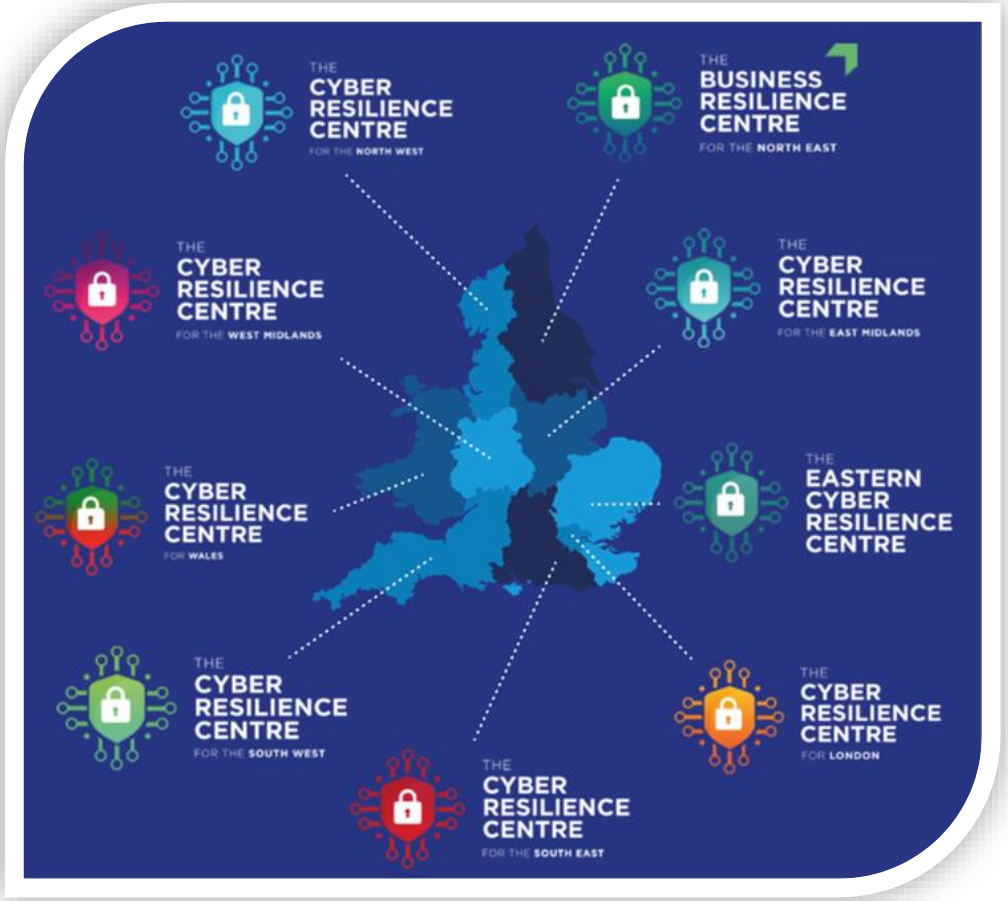
CITY OF LONDON POLICE

Prevention



The Protect & Pursue Network





National Co-ordination Office visits to all 45 forces.

Fraud Protect: 101 officers
Cyber Protect: 92 officer

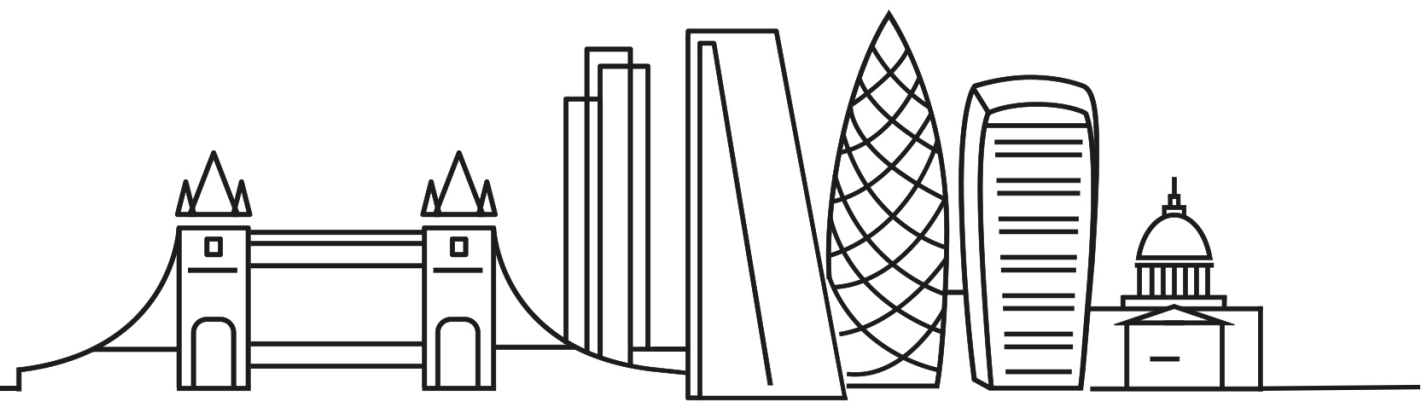
21,000 SMEs registered across CRC network.

91% of CRC engagements with companies of less than 50 employees

NECC
NATIONAL ECONOMIC CRIME CENTRE

CITY OF LONDON POLICE

Future



What Next?

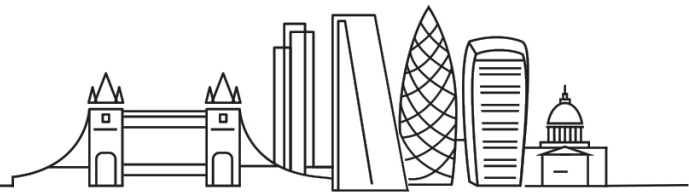
New National Fraud Strategy

Online Crime Control Centre

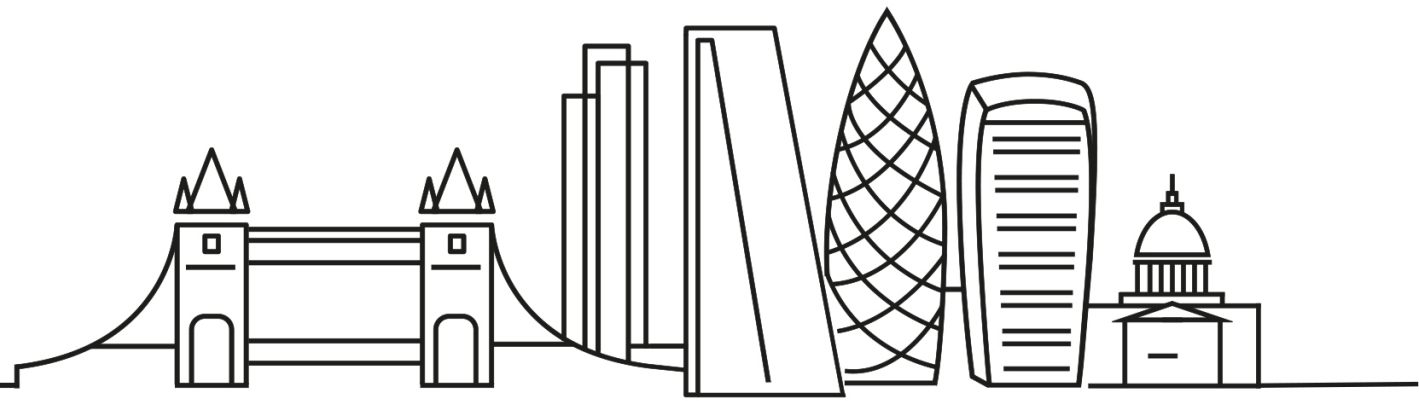
Innovation Board

CITY OF LONDON POLICE

NECC
NATIONAL ECONOMIC CRIME CENTRE



Thank you



Keynote speaker:
Luke Charters, Labour MP York Outer.

E-Crime update:
Mike Andrews, National Co-ordinator, E-Crime Team.

Introduction

- Disruption work
- Enforcement work
- How we can help you

Disruption work

- Removal of web sites and social media content
- Removal of Google content (currently fake reviews only, work ongoing re fraudulent and misleading advertising)
- DNS blocking

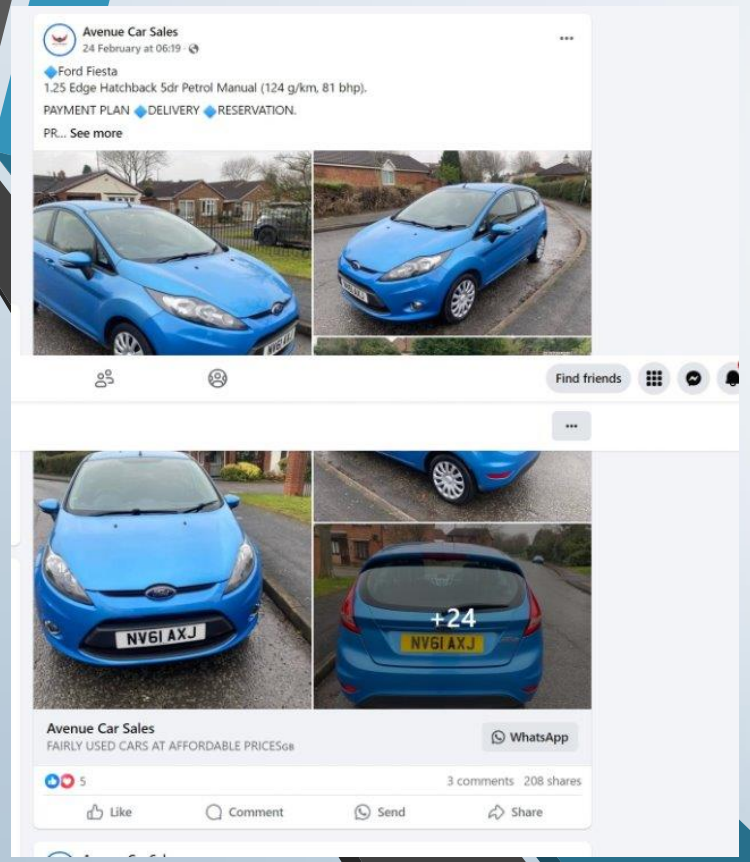
Disruption work

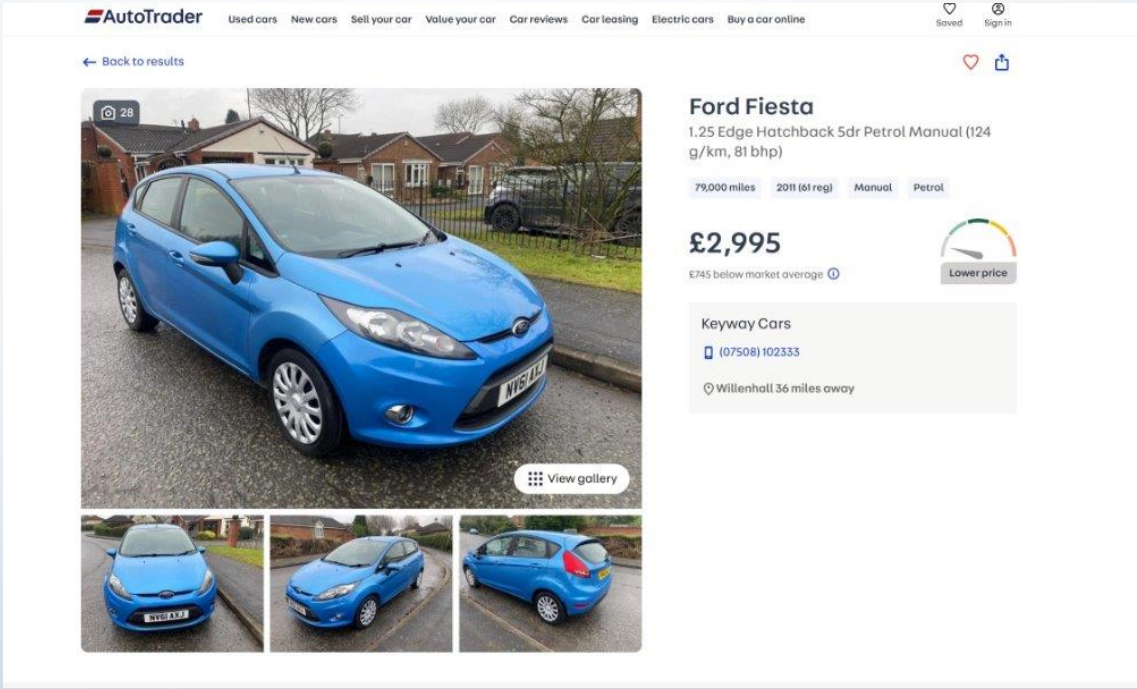
- So far dealt with over £75 million in consumer harm
- Wide range of issues from rogue trader websites through to investment frauds
- Can remove whole websites and social media profiles or specific content (where possible)

Disruption work – recent example

- Enquiry received re car dealer on Facebook
- Consumer paid £900 deposit for a car but didn't receive the vehicle
- Our enquiries revealed business address was non-existent and multiple cars we being advertised at below market price
- OSINT work revealed the ads had been 'cloned' from ads for genuine vehicles on Autotrader

Disruption work – recent example





Disruption work – recent example

- Further OSINT work revealed profiles likely being operated from outside UK
- Three profiles and over 10,000 listings subsequently identified
- All profiles and listings have now been removed

Enforcement work

- Not the solution but is still an important part of our work
- Dealt with over £250 million in harm
- Over 130 years in prison sentences
- Recovered over £20 million in criminal assets

Enforcement work – recent cases

- Operation Gilbert (yes, that one!)
- Large scale fraud centred around photography studios and modelling agencies
- Thousands of victims
- £13 million in losses identified but likely to be significantly higher

Enforcement work – recent cases

- Largely controlled by UK nationals living in Spain
- Finally concluded in February with over 24 years in prison sentences
- Extradition proceedings and POCA case now underway

Enforcement work – recent cases

- Operation Bess
- Consumers searching online for assistance with minor computer faults
- Google Ads that appeared to be for UK consumer helplines for major technology companies

Enforcement work – recent cases

- Consumers were in fact contacting call centre in India
- Conned into believing computer had major faults and were then coerced into paying as much as the call handler could extract from them
- Fronted by UK companies to avoid arousing suspicion

Enforcement work – recent cases

- Prosecuted directors of UK companies
- Five people convicted with over 14 years imprisonment
- POCA case underway
- Intelligence shared with Indian authorities

How can we help you

- Digital forensics (for cases with an online element)
  - Examination of devices
  - Online evidence review
  - On-site assistance
  - General advice

- e-learning (TSSW)
  - Basic and intermediate online investigations
  - Introduction to open-source investigations

How can we help you

- Online seminars
  - Introduction to online investigations
  - OSINT, including RIPA refresher
  - Real Deal Online scheme

- Online disruption
  - Domain suspensions/takedowns
  - Social media takedowns (currently Meta, working on TikTok)
  - Google takedowns (only fake reviews at the moment)

Break 5 mins

Communications Council UK:
Tracey Wright, Chair Communications Council UK.

Comms Council UK

- Representing over 100 telecommunications companies
- Membership represents the entire ecosystem of the sector
- Celebrating 20 years representing the advanced communications sector

What have we done so far?

- Formed a dedicated sub-group to focus on fraud prevention, detection and reporting
- Created best practice guidance for 'Know Your Customer' checks
- Created CLI guidance to ensure compliance with latest regulations
- Ongoing participation in NICC task group relating to trust in Caller ID
- Engaged with National Trading Standards to launch an information sharing initiative, alongside information sharing best practice guidance
- CCUK Fraud Summit 5th March 2025

Impact & Observations

- Member feedback indicates that KYC guidance is having a positive impact
- Ofcom enforcement programme is useful to signpost to
- CLI blocking rules are having a significant impact on internationally originated calls
- CLI blocking is causing a shift to using mobile numbers

Current initiatives

- Actively participating in Home Office Fraud Charter working groups
- Engaged with NICC CLI Task Group work looking into trace back options – the ability to trace the source of calls with spoofed numbers is key
- CCUK driving a proof-of-concept project to facilitate faster and easier data sharing – a technical solution to quickly identify the legitimate user of numbers is becoming increasingly important
- Ongoing stakeholder engagement with a focus on encouraging greater collaboration

UK Finance:

Chris Farrow, Principal APP Fraud Strategic Lead, UK Finance.

UK Finance

Authorised Push Payment (APP) Reimbursement Requirement (RR)

Chris Farrow – APP Strategic Lead

March 2025

What you need to know:



- These rules only apply to payments made on, or **after, 7 October 2024**.
- Consumers should always be careful and cautious when making payments. This means meeting the **Consumer Standard of Caution**:
- Consumers need to follow any **advice or warnings provided by their bank** and law enforcement. This may include advice on how to check that their payment is genuine, or an alert to advise that they think it may be fraud. Their bank and law enforcement will never ask consumers to transfer money to protect them from fraud.
- Consumers **must report the fraud** as soon as they can, and no more than **13 months after the last fraudulent payment was made**.
- The consumer's bank may ask them for **additional information** about their claim. Consumers need to make sure they respond to these requests.
- Once the consumer has made a claim, their bank may ask them to **report the details of the fraud to the police**, or they may offer to do this on the consumer's behalf. Consumers should consent to these steps being taken where possible and reasonable.
- The consumer's bank does not have to reimburse money lost in an APP fraud if they have shown a significant degree of carelessness (known as **'gross negligence'**) when making a payment. This would mean they would not have met the Consumer Standard of Caution.

What does the APP RR cover?



Covered:

- Payments made within the UK. Consumers are not covered for a payment sent overseas.
- Payments made using Faster Payments.
- Payments made using CHAPS.
- Payments from personal bank accounts and payments made by micro-enterprises and certain charities.
- Consumers' banks may have different rules and processes if the consumers are sending money within the same organisation. They will make consumers aware of this if the rules are different.

What does the APP RR cover?



Not covered:

- Transactions in cash, cheque, or a credit, debit, or prepaid card.
- The consumer paid using a payment system not covered under this scheme.
- It's a **civil dispute**: for example, if the consumer paid a genuine retailer or business but they aren't satisfied with the product or service they received.
- The consumer has acted fraudulently themselves – including if they have lied or misrepresented their circumstances for financial gain.
- **It's a payment the consumer made to another account that they control.**
- The payment made is unlawful: for example, if the payment was for an illegal item.
- It is a payment to and from an account with a credit union, municipal bank, or a national savings bank (state-owned savings bank in the UK).

▸ Remember, consumers may have reimbursement options under other rules, so always seek advice.

What to do if you've been scammed:



- Consumers should contact their bank immediately if they have lost money in an APP fraud. It is important that they do this as soon as they realise that they may have been scammed as delays can cause problems when trying to recover your funds.
- Consumers must report the fraud no more than **13 months** after the last fraudulent payment was made.
- The maximum amount of money consumers can claim under the rules is **£85,000.**
- Consumers' banks may ask them for information or documents to help with their claim. This could include messages or screenshots. Consumers should give them their consent to share information about the case with other banks where necessary.
- Consumers should co-operate fully with their bank when it comes to involving the police. They will help and advise consumers on how to do this based on their own ways of working.

How long will it take to be reimbursed?



- **Every claim will be assessed on a case-by-case basis.** As part of the process the consumer's bank will consider the evidence presented by them, any service providers involved and – where relevant – a third party, such as the police.
- **If the consumer's claim is valid, in most cases they should be reimbursed within five business days of making a claim.** Business days are Monday to Friday, excluding Bank Holidays.
- **In some cases, it can take up to 35 business days to be reimbursed.** This is when the consumer's bank needs extra time to gather information from the consumer, the bank that received the payment, or a statutory body (such as the Financial Conduct Authority) to inform their assessment of the case.
- **An excess of up to £100 may be deducted from any money that is reimbursed.** The consumer's bank may choose a different excess up to the maximum of £100 or not apply any excess at all. The consumer's bank will confirm the exact amount and how this will be applied.

What if the customer is vulnerable?



- There are additional protections in place for customers who, due to their personal circumstances, may be more vulnerable to being tricked by criminals. This can include a health condition, or a life event such as a bereavement.
- It could also include personal factors, such as the consumer's knowledge of financial matters, their personal financial situation, their ability to withstand an emotional shock or their levels of capability – such as literacy or digital skills.
- If these circumstances have had an impact on the consumer's ability to spot or protect themself from fraud, then they can still be reimbursed even if they did not take all the steps required under the Consumer Standard of Caution.
- The consumer's bank will also consider their personal financial circumstances when deciding how – or if - to apply an excess to their reimbursement.
- If they are a vulnerable customer there will be no excess applied.

UK Finance

Banking Protocol (Branch & Cross Channel) and Vulnerable Victims Notifications

The industry's fight against APP fraud

Banking Protocol

- The **Banking Protocol** is a rapid response scheme that enables branch staff to alert the local police when they suspect a customer is being scammed.
- Police will rapidly attend the branch, meaning they can **investigate the potential scam** and sometimes **catch fraudsters in the act**.
- The scheme helps prevent customers, particularly the **elderly and vulnerable**, from falling victim to scams.
- Since it was first launched in 2016, the scheme has led to over **1521 arrests,** prevented over **£374 million of fraud** and resulted in over **69,000 emergency calls** being responded to. Between **£5-6 million** of fraud is being prevented on a monthly basis.
- In 2024 £61.3 million was stopped through the scheme. This also led to 136 arrests



Enhancing the Banking Protocol to cover all payment channels

- Following the success of the Branch Banking Protocol, the industry then worked with national law enforcement to deliver an **on-line referral process** for scam victims identified via the on-line or telephone banking platforms – Banking Protocol Cross Channel (BPCC).
- This process provides a slower time **response to the victim's home** with a view to providing an intervention to stop the scam from taking place and to provide victim care to reduce the future susceptibility to these scam types.
- This process is designed for use with customers who, following interaction with their bank, wish to continue with the payment despite the firm's warnings that they believe this may be a scam; and who cannot attend a branch to validate the payment.

Key measures of success:

- A reduction in the number of completed frauds via the telephony / on-line channels
- The identification of vulnerable individuals, previously unknown to any of the participants.

Cross Channel Banking Protocol numbers

January – December 2023 *(2024 data is still being collected)*

- 28 financial institutions provided monthly MI returns for January to December 2023. Here are the key numbers:

- **379** BP cross channel referrals made, with **£1.7m prevented**.
- **49%** payments were not made following contact from Police/follow up from Financial Institution.
- **64%** referrals received a response from Police within the 72-hour target.

- **151** vulnerability referrals were made.

- Romance scams accounted for 26% of referrals
- Investment scams accounted for 25% of referrals

Vulnerable Victims Notifications (VVN)

- In June 2021, 7 UK Finance members commenced a 6-month Proof of Concept (PoC) with Sussex and Surrey Police, intended to empower law enforcement to share information with banks for the purpose of protecting vulnerable fraud victims from further targeting and financial loss.
- Police had identified numerous occasions where Officers and PCSOs were spending considerable time contacting victims' banks to speak with staff about introducing safeguards on their accounts and were often unable to identify the correct person or department to do this.
- Victims were being advised to self-report their fraud to their banks; however, some were unable or unwilling to do so due to their vulnerabilities.
- The Banking industry's ability to freeze funds and identify money mules was reduced due to the reliance on individuals to self-report to their bank following a fraud.
- Caseworkers, family members and Officers were assisting victims with writing lengthy complaint letters to the Financial Ombudsman detailing the vulnerabilities and rationale as to why a refund ought to be considered.
- Victims were remaining liable for losses, when had the banks been made aware of their vulnerabilities this decision could have been reconsidered.

How it works

- The VVN referrals are made following home visits initiated as part of the Op Signature process - typically by the attending Officer or PCSO but can also be made later by a fraud caseworker.
- The bank notification form, is sent by email to the relevant participating financial institution.
- The bank receives the information and takes whatever action they deem appropriate in the circumstances. This may include:
- - Contacting the customer (or family member)
- - Putting protection measures and markers on the victims' accounts
- - Making referrals to specialist vulnerability teams within the organisation
- - Blocking online banking facilities
- - Providing tailored education and awareness materials / sessions
- - Consideration of the commencement of repatriation processes/ returning funds to victims in line with the CRM code / APP Reimbursement Rules

Vulnerable Victims – Notifications from Law Enforcement

Benefits to Law Enforcement

- Officer time saved – previously, Officers and PCSOs would have to accompany victims back to their bank branch to report the fraud and request warning markers / flags.
- This process now ensures the correct department is notified directly by email immediately after the event
- Reporting the fraud to the bank no longer relies on the vulnerable victim doing so themselves, particularly when they are unable or unwilling to do so
- Notifications from Police can help influence the Bank's decision making around reimbursement and liability
- Victims are being refunded quicker - resulting in reduced vulnerability due to ongoing financial loss and emotional strain
- Considerable time savings for Officers, Caseworkers, family members and victims in cases which would previously have involved lengthy complaint processes via the Financial Ombudsman.
- Financial Institutions can apply further protections to victims' accounts including alerts, limits and warning flags, hence preventing further occurrences of fraud.
- Disruption Claim (performance measure on APMIS) for each force – 1 x moderate Protect monthly

Vulnerable Victims – Notifications from Law Enforcement

Vulnerable Victims Notification process MI

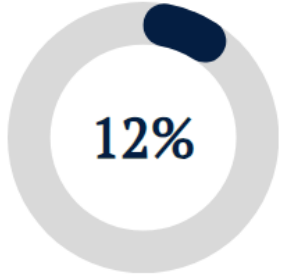
- January to December 2023 *(2024 data is still being collected)*



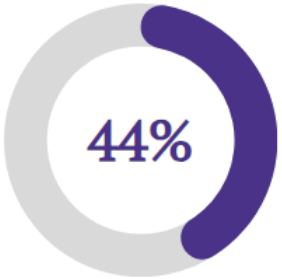
302 notifications received from law enforcement.



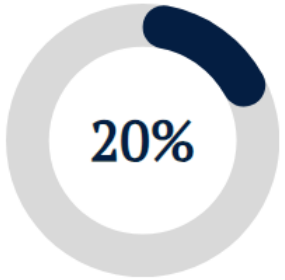
Of Vulnerable customers were flagged where the vulnerability was not previously known



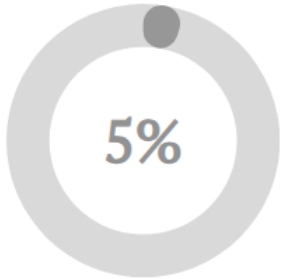
Of the total notifications received by LE have yet to be victims of fraud



Of total fraud cases received were reported as Payment fraud



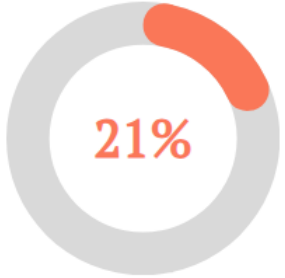
Of total fraud cases received were reported as Plastic card fraud



Of total fraud cases received were reported as Cheque fraud



Of the total fraud cases received were reported as Cash Withdrawal



Of all notifications reported were reported as "Other"

Openreach:
The digital switchover: John Livermore, All-IP Industry Engagement Manager, Openreach.

UK Analogue to Digital Switchover

John Livermore

February 2025



openreach

Openreach

A bit about us

We build and maintain the UK's largest wholesale communications network which provides phone, broadband, TV and data services to millions of homes, businesses and other organizations.

We're owned by the BT Group but we're legally separate and heavily regulated.

We work on behalf of Communications Providers like Sky, Vodafone, BT, TalkTalk, Zen and hundreds of smaller players.

Our engineers work in every community in the UK, around the clock, and in all kinds of weather to install and maintain equipment that provides fast, reliable broadband to millions of people.

We provide around 24.5m voice and broadband lines to homes and businesses in the UK.

We are upgrading the UK's broadband infrastructure to pass 25m homes and business with Full Fibre connections by 2026.

We are committed to a balanced build including over six million premises in rural and semi-rural areas.

Openreach

Communications provider

End customer

690+
Communications providers

35k+ employees

Building Full Fibre to
25m premises by Dec 2026

12.5m+ Full Fibre build complete
(2.5m rural), building 66k a week

4.2m end customers
connected to Full Fibre

The PSTN is becoming less reliable as time goes on

Ofcom Connection Nations UK Report 2023

Equipment is beyond its intended lifespan and reduced skills in legacy technology



Since 2020, the fault rate on the copper network was 50% higher than on FTTP



In 2023 the number of PSTN incidents increased by 20%



In 2023 there was a 60% increase in hours lost for customers on the PSTN



*Over the last three years, for the two operators with fibre and copper access networks (KCOM and Openreach), the fault rate (per 1,000 connections) on KCOM's copper access network (ADSL) and Openreach's copper access networks (ADSL / VDSL) was around **50% higher** than the fault rate (per 1,000 connections) on their respective FTTP networks*

Source: Connected Nations Page 64

*number of years due to the equipment being beyond its intended lifespan and reduced skills in this legacy area of technology. For instance, this year has seen a **20% increase in the number of PSTN incidents** reported to us, with a **60% increase in the amount of service hours being lost for customers.***

Source: Connected Nations Page 65

The volume of fixed incidents, particularly relating to PSTN voice, has grown over a

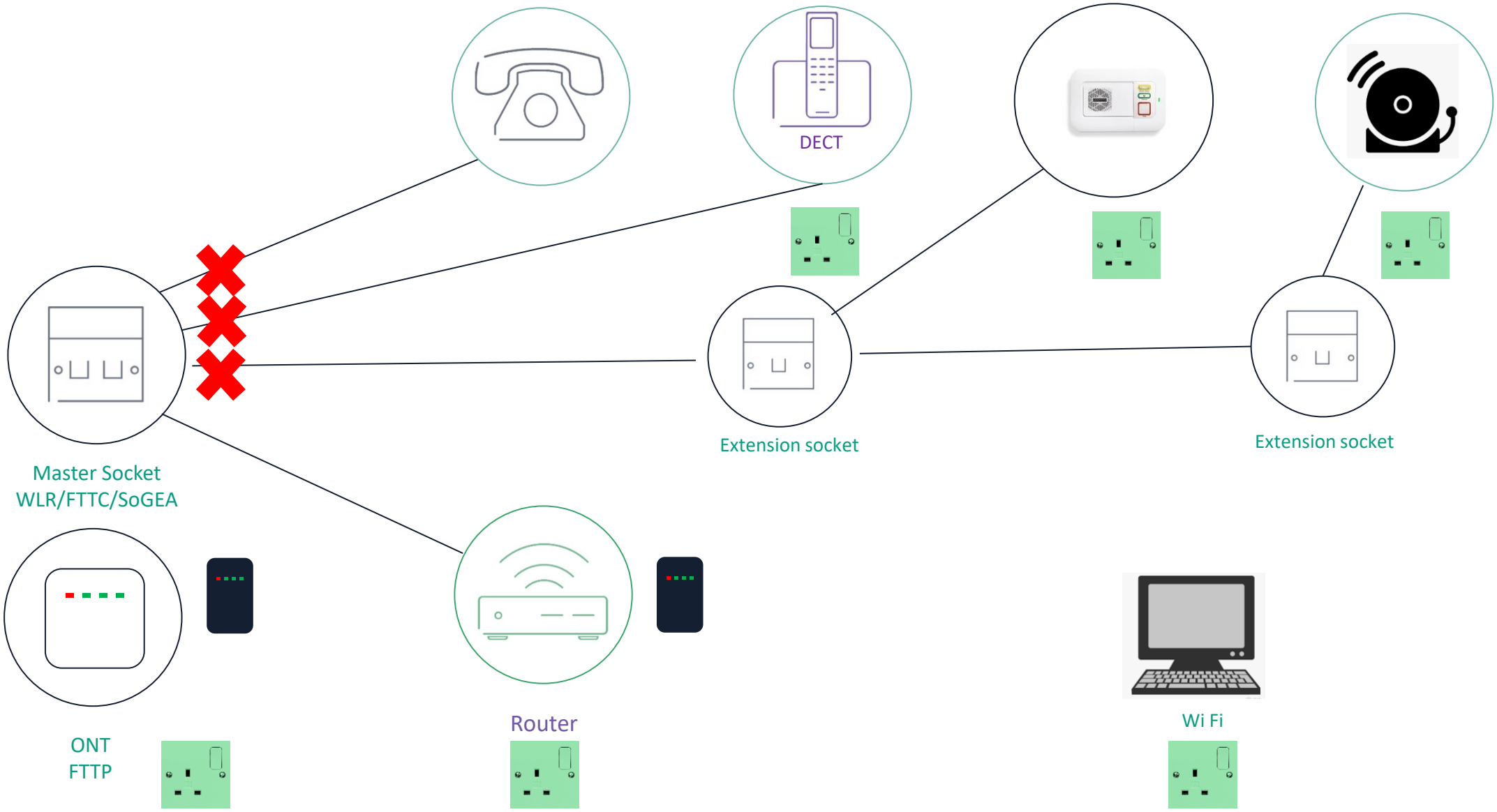
The Communications Provider

Their choices

- CPs need to move their PSTN customers from that exchange equipment before the end of **Jan 2027**
- Each CP will choose how **they** want to do this. The choices are:
- Move to **FTTP** if at the premises or **FTTC** (SOGEA) if not.
- Where there is **no Fibre** product, they can move their customer to BT Wholesale's SOADSL product (ADSL service)
- Even if Fibre is at the premises, they can move their customer to SKY or TalkTalk who have their own exchange equipment that works on an all-copper line and where there is a Special Service and the CP feels that they don't want to move their customer to Fibre. they can use BT Wholesale's PDPL (Pre-Digital Phone Line) product.
- The long-term goal should be to move to All IP on a fibre line.

So what's changing inside the premises ?

On Migration by CP to SoGEA (FTTC)/FTTP



Use Cases

- Special Services (non-standard Phone use)



Alarms
CCTV
Door Entry Systems
External Bells
Fire Alarms
Intruder/Security
Lift Alarms

Government
Custodial Tagging
Helicopter Pads
School Security
Weather Monitoring



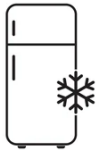
Telephony
Emergency Phones (Coastal or Bridges)
Fax Machines





Business
EPOS (Tills)
Franking Machines
Printers

Health
Baby Unit Alarms
Blood Fridges
Medical Equipment



Travel
Bus Stops
Car Park Barriers
EV Charging
Motorway Signs
Pay and Display Machines
Railway Level Crossings
Traffic Lights
Train Platform Help Points
Underground (Oyster)





Entertainment
Arcade Machines
National Lottery Terminals
Vending Machines

Monitoring
Air con units
Electricity Telemetry
Environment Agency Monitors
Flood Monitors
Gas Telemetry
Sluice Gates
Smart Meters
Streetlights
Water Telemetry



Finance
ATMs
Chip and Pin Terminals
Paypoint Machines
Stock Market Systems



Vulnerable
Telecare Alarms
Telehealth Alarms (biometrics)

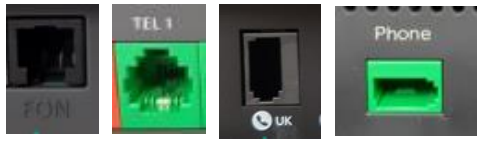


How do I connect existing devices?

All devices in the current installation will need to connect to a router supplied by their Communications Provider

There are 3 ways to connect a device to a router

1. Wi-Fi
2. Ethernet port
3. ATA port (where provided)



What is an Analogue Terminal Adapter port?

The ATA is a socket provided by SOME Communications Providers, which may be integrated into the back of the router or may present through a stand-alone device plugged into the Ethernet port on a Router

The ATA port must be “switched on” by the Communications Provider as part of the customers package

An ATA port can give very varied results and Openreach do not recommend the use of these for life saving devices

The ATA port is designed for Voice calls from phones not for sending **DTMF/STMF** tones which are machine to machine and can get lost in transmission, elongated or shortened. This could seriously affect the reliability of the devices plugged into them

Learn to C.L.A.P.

Communications

- Who is likely to receive them?
- Will they understand it?

Logistics

- Will they be able to make the changes?
- Will the router plug into the **master** socket easily?
- Will there be power available for the router/ONT?

Adjustments

- Will the CP provide an ATA port?
- Will the existing devices plug into an ATA port?
- What are the risks?

Power

- Is there power on-site?
- What will you do in a power cut situation (UPS/BBU)?

How can you get ready?

1. Audit your own telephone estate records

Check which devices you use today that are plugged into a main phone or extension socket.
This could be a telephone, a system, a telecare device, or many other things. Take the 13-month extension as a safety net, don't delay your plans.

2. Contact your device providers

Ask them how the devices will work when plugged into a router (supplied by the CP).
Do they have solutions to ensure your devices work when not using the PSTN

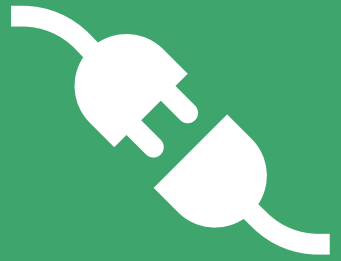
3. Contact your CP

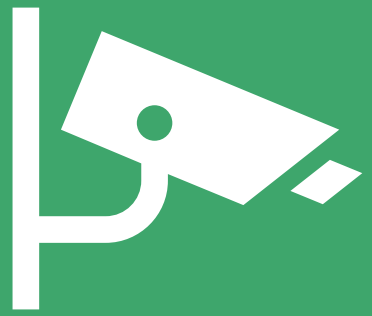
Speak to your account manager or customer services, and ask their advice for your migration.
They may have a specialist team or good information for you to read

4. Local Authorities

If you are a Local Authority, you can use a data sharing agreement to help Communication Providers identify Telecare customers in your area. https://www.local.gov.uk/our-support/cyber-digital-and-technology/digital-switchover/digital-switchover-telecare-data









Thank you

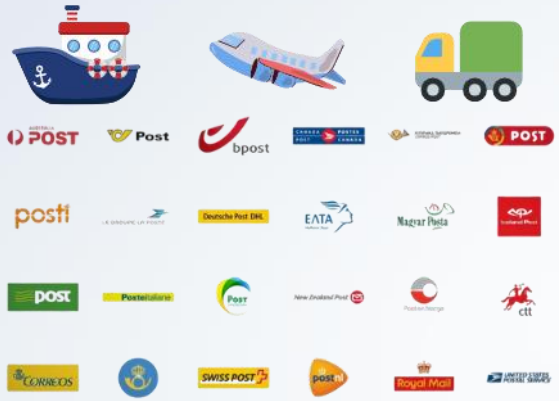
openreach

Break 55 mins

Tackling scam and nuisance calls:
Oliver Brooks-Stephenson and Richard Clarke, NTS Scams Team.

In the olden days…









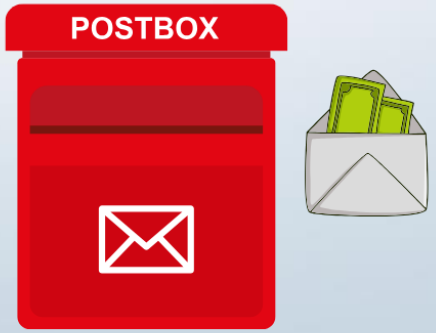












What's the problem?

- Calls still the main medium for mass marketing calls.
- A single call centre with 5-10 staff can generate seven million calls a month
- Many operate offshore to avoid UK legislation
- UK criminals use them as a one stop shop for fraud
- Technology assists the criminal.



Avatar Software used by many criminals



AI Calls –What do you think ?



Case Study

£6.6m

Following Scams Team investigation:

1,436 phone numbers removed from service

7 Call Centres identified offshore

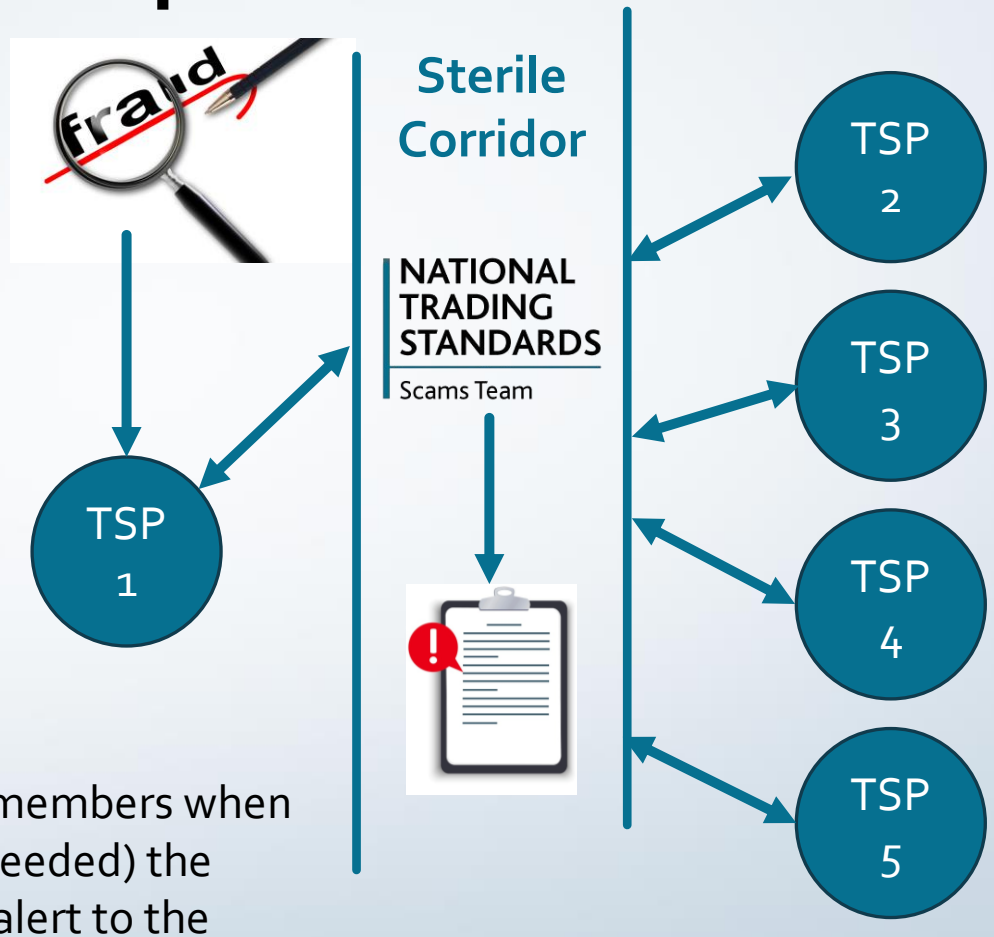
Targeting UK consumers

21,000,000 calls in a 3 month period

Estimated **£6,600,000** detriment

Alert System- UK Telco providers

We have put in place an alert system with the telecoms industry which will allow members to make an informed decision on/disengaging or sanctioning a client. All information would be anonymised and not identify a particular member



The information would be fed into us from members when they become aware. We would develop (if needed) the information and sanitise it and send out an alert to the members. We also would from our own and the wider TS family, add intelligence, alert members to new entities, practices and identifiable information to make informed decisions

The NTS Scams Team can assist you with disruption tactics if you provide us identified numbers that are suspected of being used by criminals to engage consumers.

All we ask is that the numbers have actionable intelligence to support any actions we take.

A criminal cannot operate a telephone scam without a telephone line!

Thank You for listening.



Multi Agency Approach to Fraud: Toolkit into SharePoint as a Communication Tool

Lee Ede, NTS Scams Team, David Gillies, Counter Fraud Specialist, Chair Essex Multi Agency Approach to Fraud and Charlotte Hardison, Essex Police

THE ESSEX MAAF DIGITAL HUB

NATIONAL TRADING STANDARDS Scams Team

Development of the Essex Digital MAAF.



NATIONAL TRADING STANDARDS
Protecting Consumers
Safeguarding Businesses

Multi Agency Approach to Fraud Toolkit

Objectives and Aims

- Enhance Detection and Prevention
- Support Victims
- Raise Awareness
- Strengthen Partnerships
- Improve Reporting Mechanisms
- Utilize Technology
- Streamline Communications between Agencies

- Focus on enhancing fraud protection and safeguarding vulnerable victims
- Bringing together resources and expertise from both public and private sectors, to raise awareness and provide clear, unified guidance on fraud prevention
- Ensures a more effective approach to combating fraud and protecting those most at risk

Policy Alignment

CITY of LONDON POLICE

National Policing Strategy for Fraud, Economic and Cyber Crime 2023 - 2028





THE ESSEX MAAF DIGITAL HUB

VS
VICTIM SUPPORT







SAFER ESSEX



Design Considerations

- Accessibility
- Efficiency
- Adaptability
- Training and Awareness
- Data Integration
- Existing Microsoft Technologies
- Enhanced Security
- Cost
- Communication

"Holistic multi-agency, situational driven support service."



Notable Achievements

Improved Data Sharing

- The collaborative approach has enhanced the timely sharing of data between partners, improving decision-making and allowing for better-targeted campaigns and fraud prevention messaging interventions.

Establishment of a Multi-Agency Hub

- Combines resources, expertise, and intelligence from local authorities, Essex County Fire and Rescue Service, Trading Standards, Victim Support Essex, Adult Victim Services, and local volunteer groups. Significantly improves efficiency and effectiveness in fraud prevention.

Successful Fraud Interventions

- Swift action by the Economic Crime Team led to the arrest of two suspects exploiting an elderly woman through rogue trading. Highlights the importance of rapid response and collaboration among agencies through the MAAF.

Successful Fraud Interventions

- The Romance Fraud Peer Support Group offers emotional relief and practical advice. Over 200 victims helped, with some becoming mentors and advocates. Part of a broader collaboration among support services for comprehensive assistance.

Public Fraud Prevention Awareness Campaigns

- MAAF has initiated joint local and national campaigns with unified media messaging. In 2024, these campaigns reached over half a million residents, significantly increasing community awareness and engagement, and helping to prevent fraud before it occurs.

Challenges

- Data Sharing
- Training and Capacity Building
- Feedback and Continuous Improvement
- Collaborative Efforts
- Implementation Plan Design

Power of Language:

Dr Elisabeth Carter, Associate Professor of Criminology, Forensic Linguist and Vice President of the International Association of Economic Criminology.

Romance Fraud: Manipulation, Protection and Prevention



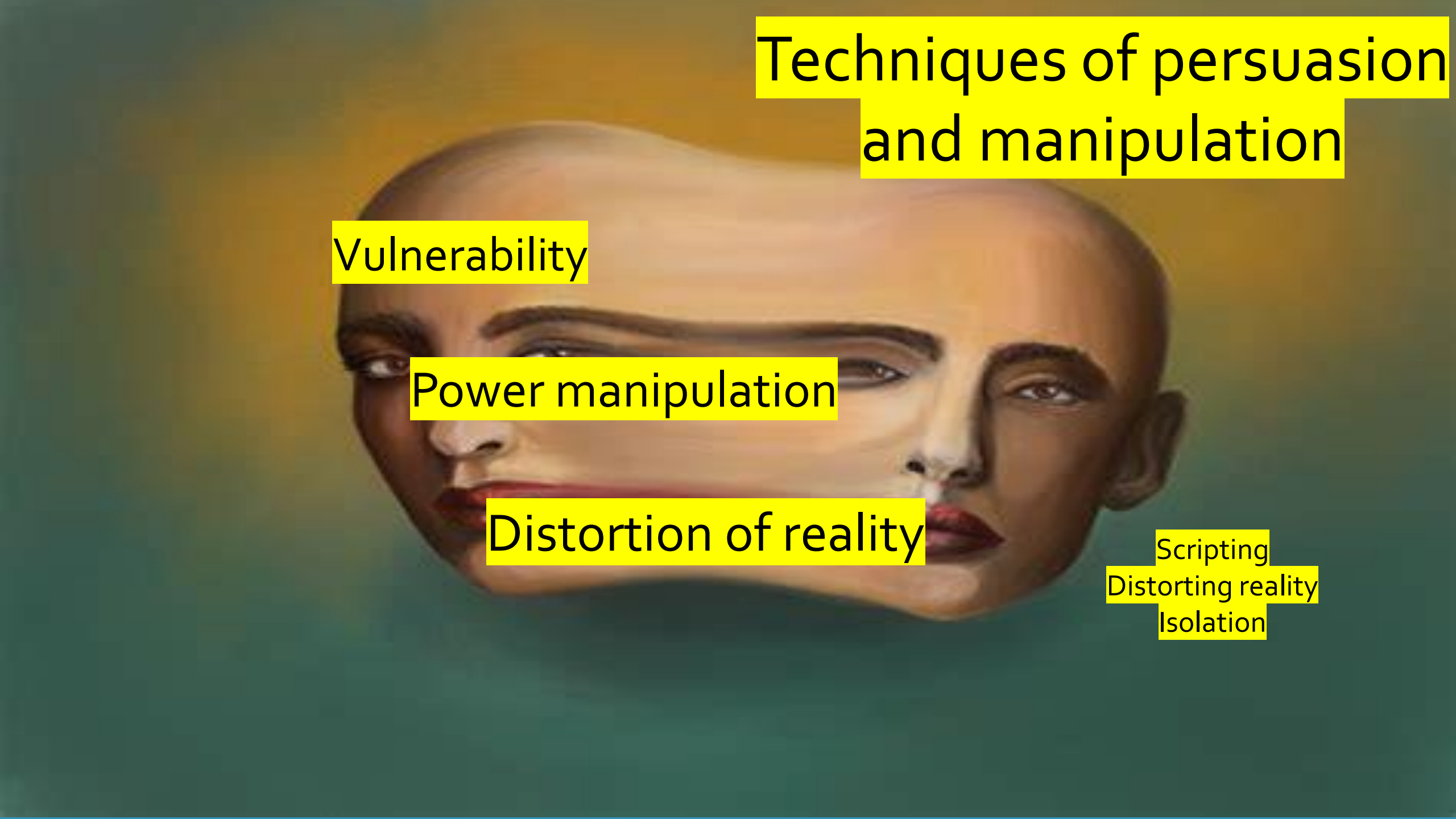
Dr Elisabeth Carter
Criminologist and Forensic Linguist
Kingston University, London
E.Carter@Kingston.ac.uk

Romance fraud

- Active participation of victim
- Harms go beyond the financial
- Negative narratives specifically around older victims



Techniques of persuasion and manipulation



Vulnerability

Power manipulation

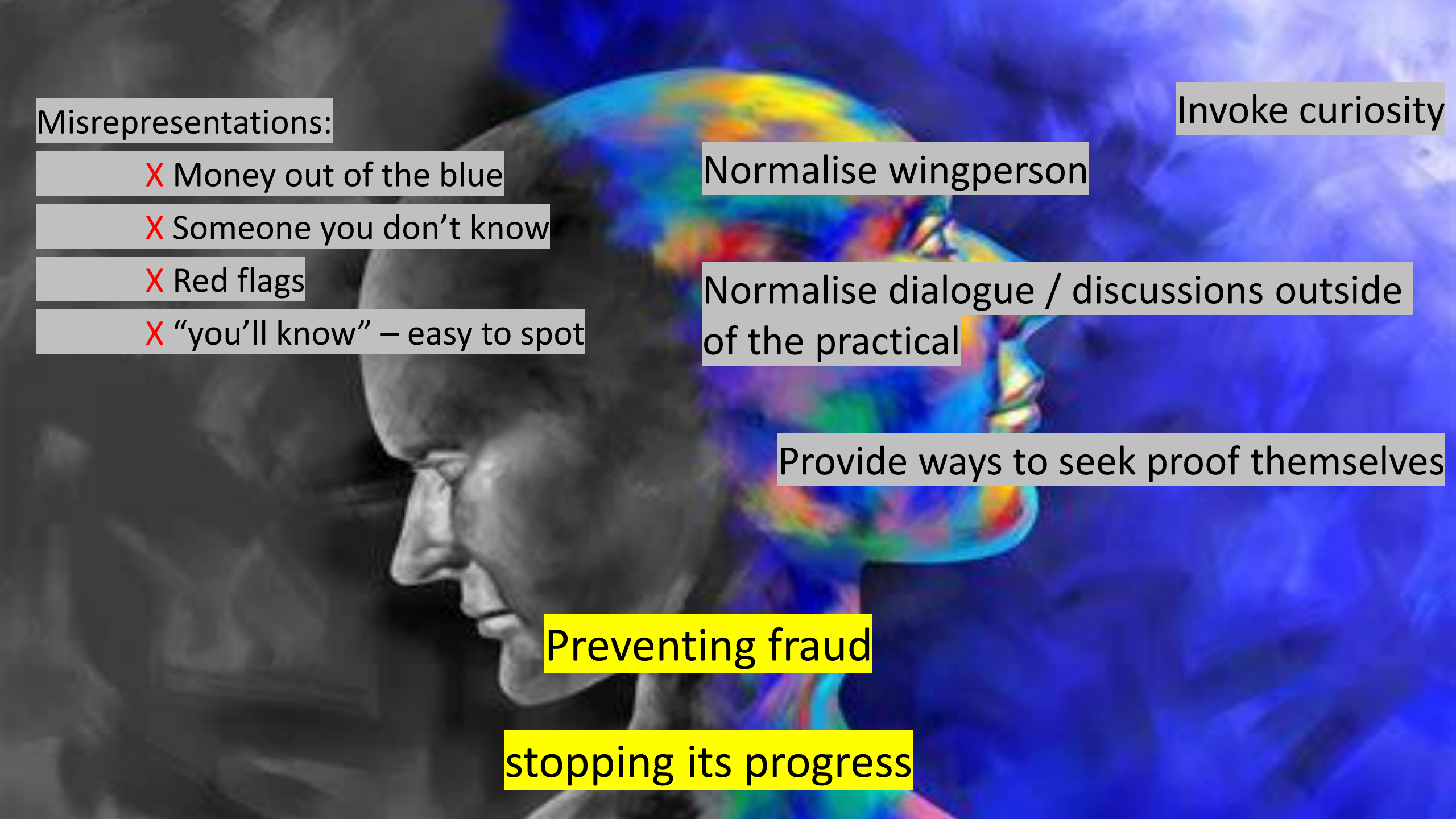
Distortion of reality

Scripting
Distorting reality
Isolation



Prevention and protection

- Coercion without concern
- Joint enterprise
- Responsibility
  - For health of relationship
  - For well-being of fraudster
- Leveraging love and fear
- Future prospects
- Scarcity
- Self-doubt


Misrepresentations:
X Money out of the blue
X Someone you don't know
X Red flags
X "you'll know" – easy to spot
Invoke curiosity
Normalise wingperson
Normalise dialogue / discussions outside of the practical
Provide ways to seek proof themselves
Preventing fraud
stopping its progress

Print ISSN 0007-0955 Online ISSN 1464-3529

BJC

THE BRITISH JOURNAL OF
CRIMINOLOGY

AN INTERNATIONAL REVIEW OF CRIME AND SOCIETY

VOLUME 61 NUMBER 2 MARCH 2021

Published on behalf of the Centre for Crime and Justice Studies
in association with the British Society of Criminology

https://academic.oup.com/bjc

OXFORD
UNIVERSITY PRESS

NATIONAL
TRADING
STANDARDS
Scams Team

National Trading Standards (NTS) Scams Team 'Coercion and control in financial abuse; learning from domestic abuse'

October 2022

Authors:

Jennifer Hawkswood
Dr Elisabeth Carter
Professor Keith Brown

Print ISSN 0007-0955 Online ISSN 1464-3529

BJC

THE BRITISH JOURNAL OF
CRIMINOLOGY

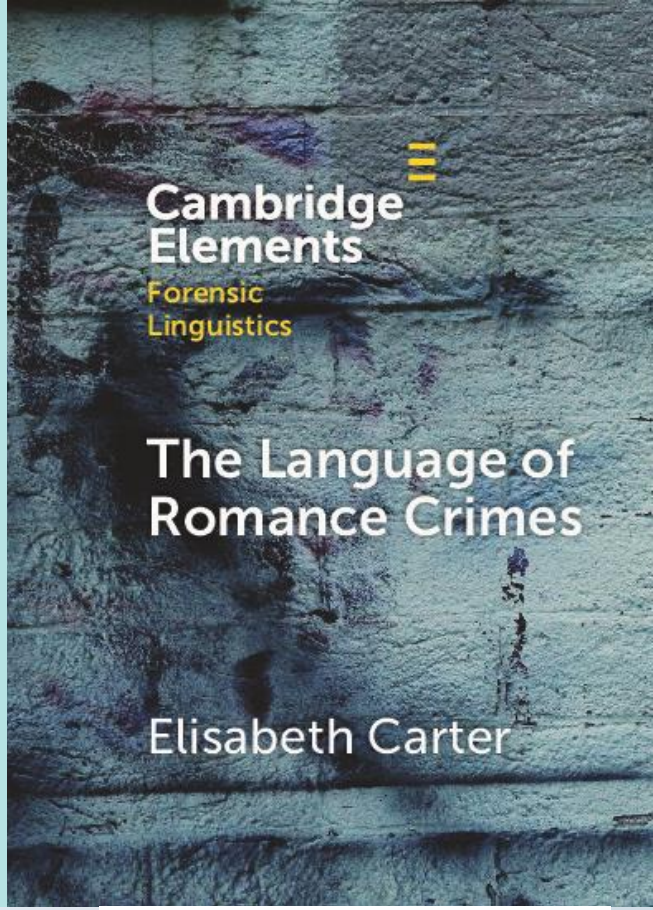
AN INTERNATIONAL REVIEW OF CRIME AND SOCIETY

VOLUME 63 NUMBER 6 NOVEMBER 2023

Published on behalf of the Centre for Crime and Justice Studies
in association with the British Society of Criminology

https://academic.oup.com/bjc

OXFORD
UNIVERSITY PRESS



Romance Fraud: Manipulation, Protection and Prevention



Dr Elisabeth Carter
Criminologist and Forensic Linguist
Kingston University, London
E.Carter@Kingston.ac.uk

Break 5 mins

Economic Abuse:
Samantha Beckinsale, The Love Project.

Digital Markets, Competition and Consumers Act 2024: Clare Forbes, NTS Scams Team.

Fraud Fighters: Using the DMCCA to Combat Consumer Scams

Key Changes to consumer protection from unfair practices in the Digital Markets, Competition and Consumers Act 2024



What is the DMCCA?

- **Biggest reform in consumer law in years**
- Strengthens **enforcement powers for Trading Standards & Competition and Markets Authority**
- Tougher rules on **misleading practices, aggressive selling & scams**
- **New direct penalties** – up to **10% of global turnover**

Part 4 Consumer Rights & Disputes

Key changes:

- Definitions
- Reworded and re-ordered Prohibited Practices – Sch 20
- Widened scope of misleading actions and omissions
- New offence for omitting information in an invitation to purchase
- Removal of restrictive elements of aggressive practices and professional diligence

What is unfair?

A commercial practice is unfair if…

"it is likely to cause the average consumer to take a transactional decision that the consumer would not have taken otherwise…"

- Misleading actions, omissions, aggressive practices or contravening the requirements of professional diligence

It omits information from an invitation to purchase

It is listed in Sch 20

Average Consumer

Group is particularly vulnerable to a practice, and the trader can reasonably foresee

- **Nature of the product**
- Age
- Physical or mental health
- Credulity
- **the CIRCUMSTANCES they are in**

Likely to cause them to take a transactional decision they wouldn't have taken otherwise

Average Consumer: Vulnerable persons

Group is particularly vulnerable to a practice, and the trader can reasonably foresee

- **Nature of the product**
- Age
- Physical or mental health
- Credulity
- **the CIRCUMSTANCES they are in**

Likely to cause them to take a transactional decision they wouldn't have taken otherwise

Sch 20 Prohibited Practices

Current practices

- Approvals, logos, codes and endorsements
- Bait advertising & bait & switch
- High pressure limited time / price, scarcity or market conditions
- Pyramid schemes
- Prize draws and competitions
- "Free" products – subscription traps
- Fake invoices/demands for payment
- Ignoring request to leave/not return to consumers home
- Persistent telephone (or other) contact

Amended/new practices

- Para 13 –Submitting, commissioning or publishing fake reviews (civil enforcement only)
- Para 14 – risks to the personal security **or safety** of the consumer/family etc
- Para 19 – false claims that product can **prevent or treat** disease/malformation (body or **mind**), **restore, correct or modify physiological function, or modify a person's appearance**

Omitting material information in an invitation to purchase

- Now a separate offence – no transactional decision/average consumer test
- Material information required:
- Main characteristics
- Total price / manner in which price will be calculated
- Identity, business address & email of the trader and any other trader they are acting on behalf of
- Freight/delivery/postal charges
- Withdrawal or cancellation rights
- Any difference from traders published practices relevant to the commercial practice
- Any legally required information

Misleading actions and omissions

False or misleading information regarding:

- The trader
- The product
- Anything else relevant to the transactional decision

List of matters removed

Omitting:

- Material information
- Legally required information
- Commercial intent

Unclear, untimely or in a way that consumer is unlikely to see it

Aggressive practices

- Harassment
- Coercion
- Undue influence

Nature of the practice	Timing and location	Threatening or abusive language or behaviour
Exploiting a vulnerability	Threats to take legal action	Onerous or disproportionate actions to exercise rights

Professional diligence

Practice falls short of standard of care and skill expected

Honest market practice

General principle of good faith

Knowingly or recklessly….

Friends Against Scams and Doorbell project: Adam Carter, NTS Scams Team.

Questions and close