

Monthly Threat Update

North East Economic & Cyber Crime

Welcome to the Monthly Threat Update (MTU) from NEROCU. This document provides an overview of Economic and Cyber crime trends within the North East and UK.

This document contains August 2026 data with a forward outlook.

Please contact the Regional Economic Crime Coordination Centre (RECCC) if you have any questions: RECCC@durham.police.uk

Reading Time 5-10 minutes.

Contents

Looking Back



- Regional Cyber Summary
- Regional Fraud Summary
- Engagement Events

Contents

Looking Forward



- Horizon Scanning
- What's Happening Next

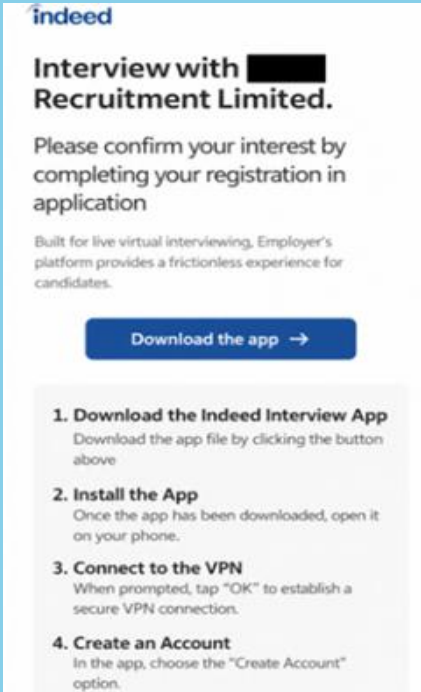
North East Cyber Crime August Summary

 **34% THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR**

Total Cyber Reports (compared to August 2025)		 101 (-34%)
	Hacking -Social Media and Email	 65 (-48%)
	Hacking - Personal	 22 (+22%)
	Computer Virus/ Malware	 7 (+250%)
	Hacking - Extortion	 2 (-75%)
	Hacking – PBX/ Dial Through	 3 (-%)
	Denial of Service Attack	 0 (-%)

Fake Indeed Interview Applications used to install Spyware

Scammers are using fake Android “interview” apps to target job seekers on the Indeed platform. The scammers trick applicants to download the malicious interview tool app that is not affiliated with the legitimate Indeed job search platform. It works by scammers advertising fake job openings on Indeed and prompts applicants into installing a fake Android App that impersonates Indeed and is advertised as an interview tool. The applicant receives instructions like the below:



Once the Malware is on the device and granted the Accessibility permission it takes control of the device.

Protect yourself against job scams:

The interview process on the legitimate Indeed platform does not require users to download interviewing apps, the entire process happens within the official Indeed browser.

The official Indeed Job Search app is distributed through Google Play and not through links or unfamiliar interview website.

Any message asking a job seeker to download an app to participate in an interview is a scam. A job interview should not require you to download an app outside of the official play store, enable a VPN or install unknown software. Do not click any links or download files.

Also verify job offers through independent channels and complete due diligence on the company as in some cases, the company did not exist.

North East Fraud August Summary



**LOWER THIS MONTH
THAN THE SAME MONTH
LAST YEAR**

Total Fraud Reports (compared to August 2025)		 670 (-15%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:		
	Advance Fee Frauds Cheque, Plastic Card and Online Bank Accounts	 134 (-0.74%)
	Online Shopping and Auctions	 127 (+0.79%)
	Cheque, Plastic Card and Online Bank Accounts	 90 (+131%)
	Investment Fraud	 68 (+4.6%)
	Other Consumer Fraud	 33 (-57.7%)

Note: the large increase in **Cheque, Plastic Card and Online Bank Accounts** is due to changes in national data recording with new data sources included

Disaster-Related Donation Fraud Risks

The recent flash flooding in Nepal is likely to create opportunities for fraudsters to exploit public sympathy through fraudulent donation appeals.

Criminals create fake causes based on real disasters covered in the media to attempt to persuade individuals to donate by leveraging the urgency and emotional impact of the disaster.

It is not just International disasters exploited in this way, criminals are also known to create fake crowd funding pages raising money for local charities or those in need locally.

Common tactics include fake charities, impersonation of legitimate aid organisations, and unsolicited donation requests distributed via email, calls, text message, social media, and messaging platforms. Fraudsters may also use AI-generated imagery and fabricated stories to increase the credibility of fraudulent campaigns. They have also been known to use real photos of poorly children stolen from their parents social media accounts.

Anyone wishing to donate to charity appeals should verify the charity and check if the organisation has an official Registered Charity Number by searching the [UK Charity Register](#).

Genuine online crowdfunding pages usually link directly to an established, verified charity profile on the platform rather than a personal bank account

Look for the Fundraising Regulator badge on their website or materials, signifying adherence to the Code of Fundraising Practice

Online Shopping Fraud

What it is...a criminal selling you something that doesn't exist or a buyer offering you money they are not going to send



HOW TO STOP IT

Check Websites - Check Adverts

How to spot a fake Online Advert &
How to spot a fake Website are on...

www.stopthinkfraud.campaign.gov.uk

AND

Use the National Trading Standards APP

Friends Against Scams

Be wary if anyone:

- asks you to share a one-time-passcode
- asks for your PIN or password in full
- asks for payment before sending a prize or lost delivery
- asks for a direct transfer of cash or cryptocurrency
- asks you to move away from an official payment site to make a direct payment
- asks you to send gift cards
- asks for money before you've met in person
- asks you to click on suspicious links

HOW TO STOP IT

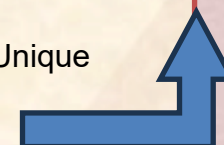
Cyber Hygiene

Ensure Passwords are Long Strong & Unique

Use www.security.org

Activate Two-Step Verification on ALL your email and social media accounts

Keep your devices
& anti-virus updated



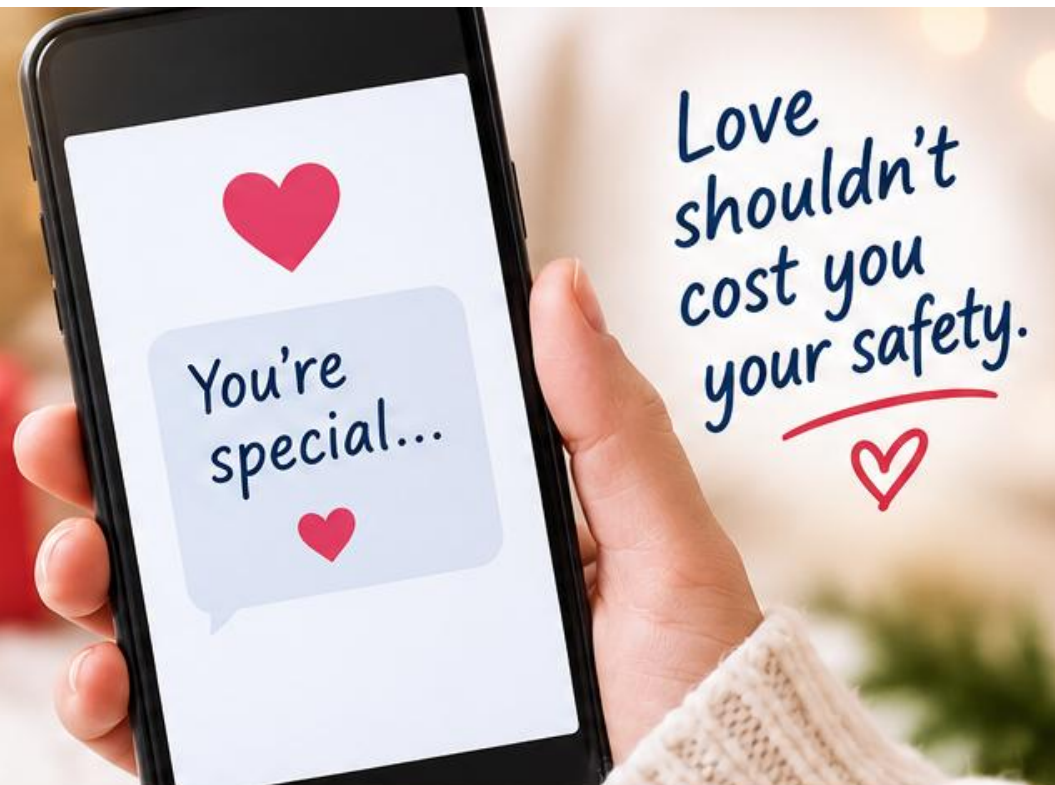


International Romance Fraud Prevention Day

Real love doesn't ask for money.

On October 3rd, we raise awareness about romance fraud — a growing crime where scammers build fake relationships to steal money and personal information.

Be informed. Stay alert. Protect your heart (and your wallet).



Watch for the warning signs:



Fake profiles

Scammers often use stolen photos and create multiple accounts.



Too good to be true

They may quickly declare love, make big promises or ask for money.



Requests for money

They may ask for financial help, gift cards, or payment for a “good opportunity”.



Pressure and secrecy

They may discourage meeting in person or keep the relationship private.



Do your research

Verify their identity, check for red flags and trust your instincts.

Engagement Events

This month we have visited and worked with:

- ✓ Cleveland Retail Crime Forum
- ✓ Seaham U3A
- ✓ Castles & Coast Housing
- ✓ St Teresa's Hospice Darlington
- ✓ Age UK Durham
- ✓ Citizens Advice Gateshead
- ✓ Northumbria University
- ✓ Teesdale Valley Day Clubs
- ✓ Lloyds Halifax Banking Group



Do you want to be a part of our growing Fraud Protect Community?

Contact us at:

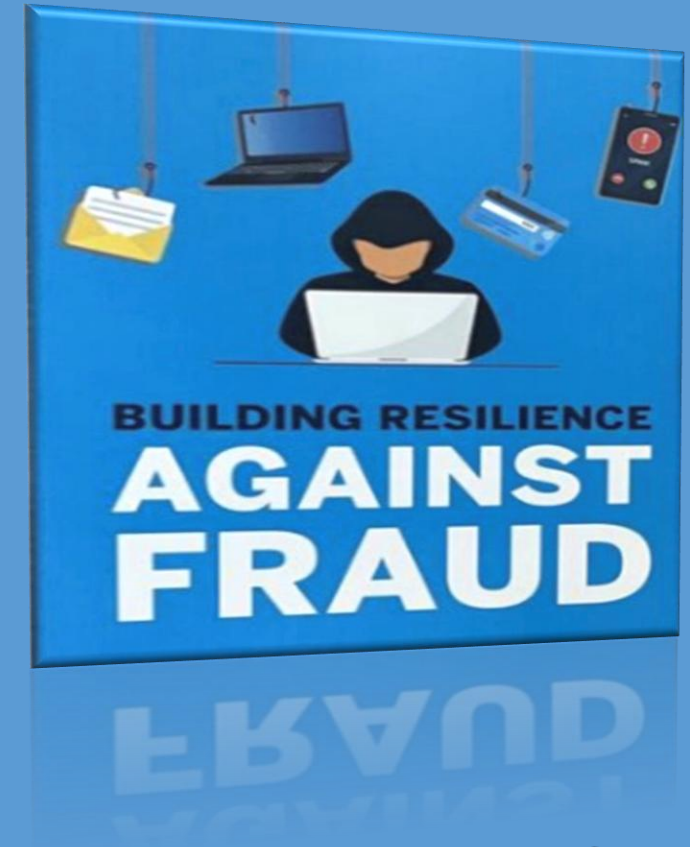
RECCC@durham.police.uk



What's Happening Next?

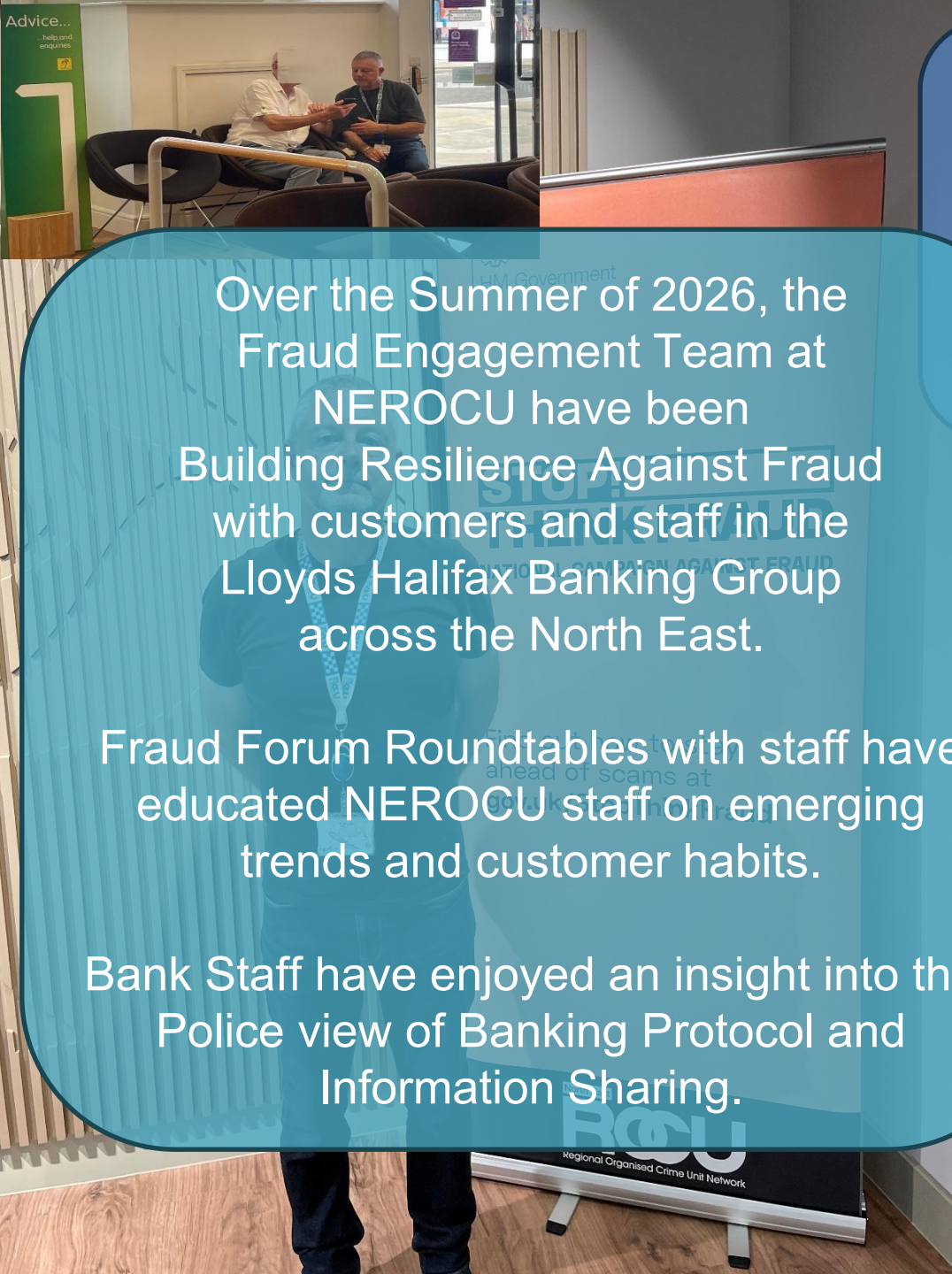
Regional Events:

- ✓ Fraud & Scams Talks and Fraud Protect Roadshow at Gateshead Business Expo
- ✓ Fraud Watch Roadshows at Lloyds & Halifax Banks – check your local branch for info
- ✓ Fraud Watch Roadshows at Fresher's Events at the Further Education Providers: Darlington College, Prior Pursglove 6th Form, Middlesbrough College & Sunderland College (Bede & City Campus) and North Tyneside College
- ✓ Fraud Watch Roadshows at Fresher's Events at the following Higher Education Providers: Durham University, University of Sunderland, Northumbria University, Newcastle University and Northern School of Art
- ✓ Fraud Watch Roadshow Events with Pride in Place TS6
- ✓ Digital Inclusion with Miners Lamp in Prudhoe
- ✓ Cyber Security Awareness Month in October



If you'd like further information or would like to invite the RECCC to your event, please email us at: RECCC@durham.police.uk

We are happy to help where possible to facilitate a strong and engaged North East Network



Partnership Working: Lloyds Halifax Banking Group

Over the Summer of 2026, the Fraud Engagement Team at NEROCU have been Building Resilience Against Fraud with customers and staff in the Lloyds Halifax Banking Group across the North East.

Fraud Forum Roundtables with staff have educated NEROCU staff on emerging trends and customer habits.

Bank Staff have enjoyed an insight into the Police view of Banking Protocol and Information Sharing.

Fraud Watch Roadshows have been held for customers in:

North Shields
Hartlepool
Wallsend
Durham City
Redcar
Stockton-On-Tees
Newcastle-Upon-Tyne
Middlesbrough
Consett



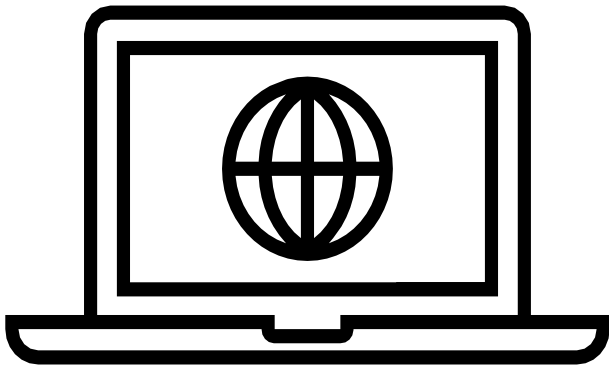
Do you want to know more about Fraud Forum Roundtables and Fraud Watch Roadshows for your Bank?

Contact us at:

RECCC@durham.police.uk

Horizon Scanning

Monitoring Threats



Black Friday Sales

Black Friday is looming, scheduled to begin November 27th, and some retailers offer pre black Friday deals. Criminals target shoppers through fake websites, unbelievable discounts, phishing emails, text messages and unusual payment requests. Always check seller and website addresses, avoid clicking on unsolicited links, never share passwords or security codes and don't let pressure tactics rush your decisions.

Beware fake, seasonal jobs

Fake seasonal and Christmas job adverts will be coming soon, targeting those wanting extra income for the festive period. Criminals advertise jobs that don't exist, promise high wages for little or easy work and/or ask for upfront fees to be paid along with providing personal and banking information. Verify employers through official websites, never pay to secure a job, never trust unsolicited offers and avoid sharing sensitive information.

As always – if you receive an unexpected text / call / email, treat it with suspicion and do not trust it. Never click on a link. Verify any information via trusted means.

Think SCAM –

Stop – take 5 minutes

Check – look at the details

Ask – ask trusted people

Manage – report the issue to report fraud or police.





 For more information search 'nerccu police'



BUILDING RESILIENCE AGAINST FRAUD

How to report



Police

All Fraud in the UK is reported to the police at Report Fraud by phone or online:
www.reportfraud.police.uk
0300 123 2040

Report Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Report Fraud



Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline)
An automated line which Takes you through to your Bank's Fraud team .

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



Phone Numbers

Forward phone numbers Sending you Fraudulent Messages or calls to **7726**



Police-Led, Business Focused
Here to protect businesses from online fraud
and cybercrime



**Supporting Sole traders, Micro, Small and
Medium businesses, charities and standalone
schools**

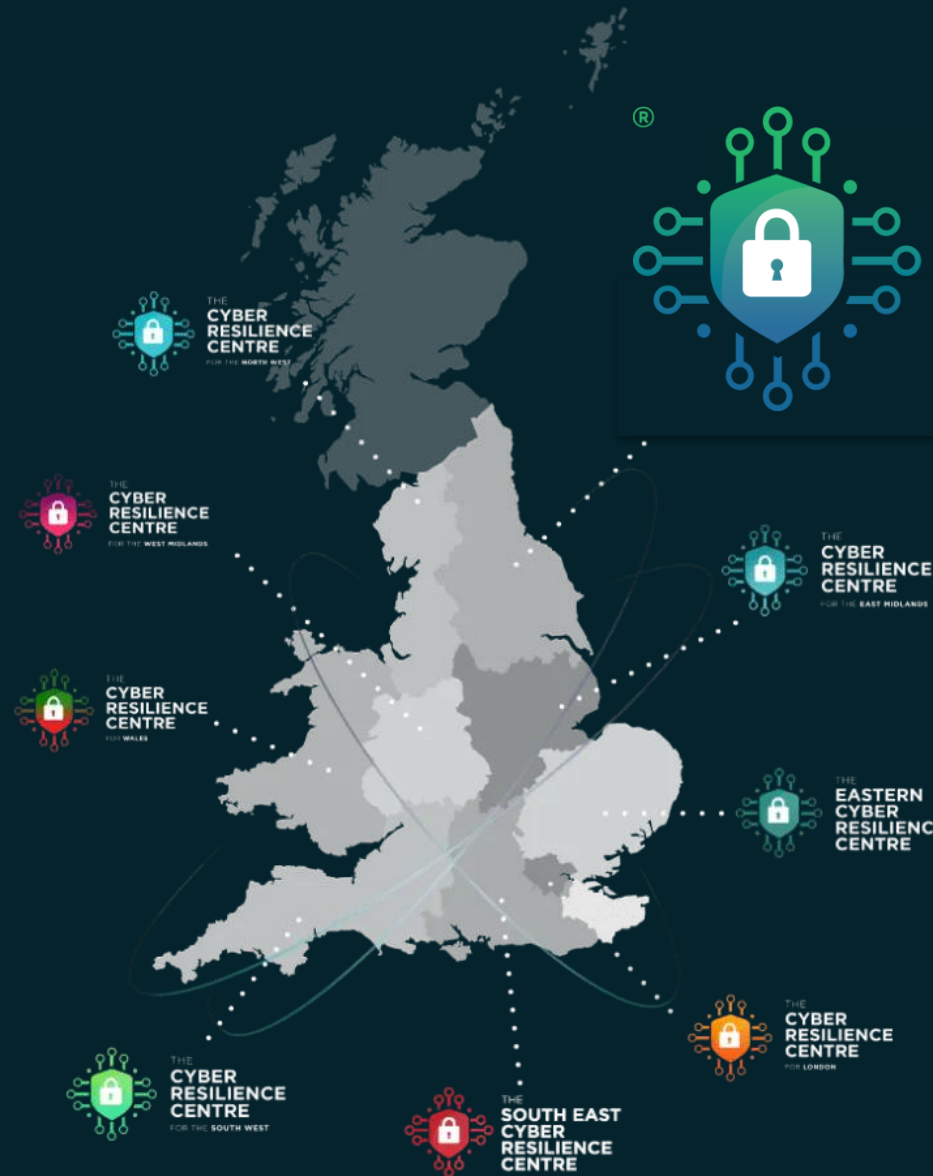


National Network of 9 Centres



Fully funded services:

- Free membership
- Monthly newsletter with tips and guidance
- Cyber security services
- 1-2-1 Support
- Links to Policing
- National Cyber Security Centre (NCSC) Resources



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE NORTH EAST
YORKSHIRE | THE HUMBER

**Join your local
CRC, the North
East Centre:**



Handling Instructions

Distribution List
NEROCU
North East Police Forces

Copyright © NEROCU 2025 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this document, it is provided in good faith on the basis that NEROCU and its staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to NEROCU. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this document, please contact NEROCU. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

Provenance: Available upon request.



Protective Marking	Official – Law Enforcement
Version	Final
Purpose	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.
Owner	NEROCU
Authors	Claire Hardy – Economic Threat Desk Analyst Nicola Lord – Cyber Threat Desk Analyst PC Brian Collins – Engagement Officer PC Andy Hampson – Engagement Officer
Reviewed By	Sgt Paul Mann

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by NEROCU in confidence and may not be shared other than with the agreed readership/handling code without prior reference to NEROCU. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018. The cover sheets must not be detached from the report to which they refer.