SUFFOLK CONSTABULARY

ORIGINATOR: CHIEF CONSTABLE	**PAPER NO: AP26/42**

SUBMITTED TO:	**ACCOUNTABILITY AND PERFORMANCE PANEL - 4 SEPTEMBER 2026**

SUBJECT:	**CRIME, SAFEGUARDING & INCIDENT MANAGEMENT (CSIM)/ COUNTY POLICING COMMAND – RESPONDING TO FRAUD**

SUMMARY:

1. This report outlines Suffolk Constabulary's strategic and operational response to fraud, highlighting key developments, performance trends, and future priorities. It reflects alignment with national directives including the National Fraud Strategy, Strategic Policing Requirement (SPR), and HMICFRS inspection framework. The report identifies strengths in victim support, multi-agency collaboration, and capability development, while also acknowledging challenges in investigative outcomes and resource constraints.

RECOMMENDATION:

1. The Police and Crime Commissioner (PCC) is asked to consider the contents of this report and progress made by the Constabulary and raise issues with the Chief Constable as appropriate to the PCC's role in holding the Chief Constable to account.

DETAIL OF THE SUBMISSION

1. INTRODUCTION

1.1. During this reporting period, Report Fraud replaced Action Fraud as the national reporting route for fraud and cybercrime. The National Economic Crime Victim Care Unit is now known as Report Fraud Victim Services (RFVS).

1.2. This report covers fraud performance data during the period of 1st July 2025 until 30th June 2026.

1.3. This paper supports the Police and Crime Plan commitment which states that the Constabulary will strengthen its approach to fraud investigation, prevention, and victim support.

1.4. The strategic management of fraud is delivered by the Detective Chief Superintendent of Crime, Safeguarding and Incident Management (CSIM) with operational delivery being within Workflow Management and Investigations departments. Chief Officer oversight of fraud delivery is provided by T/Assistant Chief Constable Paul Wells. A Fraud Improvement and Delivery board is chaired by the Detective Chief Inspector Workflow Management, providing tactical delivery of development and improvement.

2. FRAUD PERFORMANCE

2.1. The performance data presented is taken from Power BI, where all Constabulary fraud data can be accessed. Performance data in Power BI is recorded from 1 August 2021 and encompasses data from the National Fraud Intelligence Bureau (NFIB).

2.2. There are three primary classifications of fraud encapsulated within the data presented:

- Report Fraud Call for Service – Investigations reported directly to the Constabulary where the offence has occurred in Suffolk, and the suspect is also based in Suffolk.
- Report Fraud NFIB Referral - Investigation allocated to the Constabulary by the National Fraud Intelligence Bureau after their assessment of a Report Fraud submission. Referral indicates the case has been developed to the point where a viable suspect has been identified within our policing area, and the Constabulary is responsible for progression.
- Non-crime Financial Investigation – Investigations reported directly to the Constabulary when suspects are unknown or not within Suffolk. This would include frauds where it is apparent the suspect is not within the UK and NFIB vulnerable person notices.

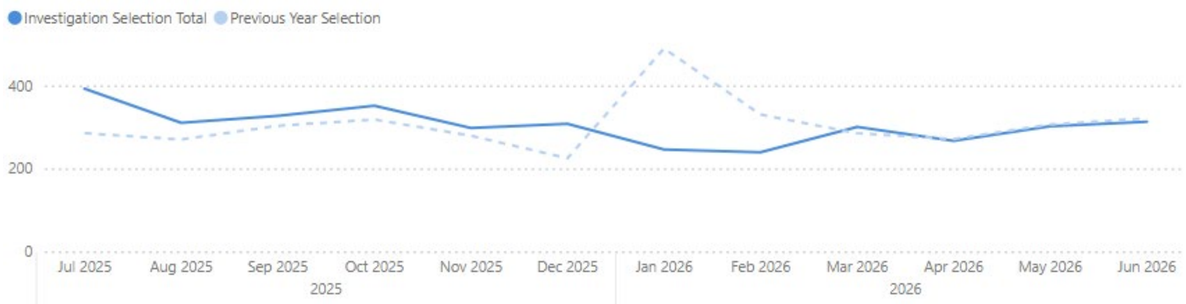
2.3. Data collation in Power BI, enables illustration of four full years of the same metrics captured. Subsequently, this is shown in a table format, below. Please note that due to the start of data collation the first period is ten months (1 August 2021 to 30 June 2022). The data is presented in this way to show like-for-like comparisons, which can consistently be reported on for future reporting periods.

Table 1, below, shows the data for the three primary fraud classifications:

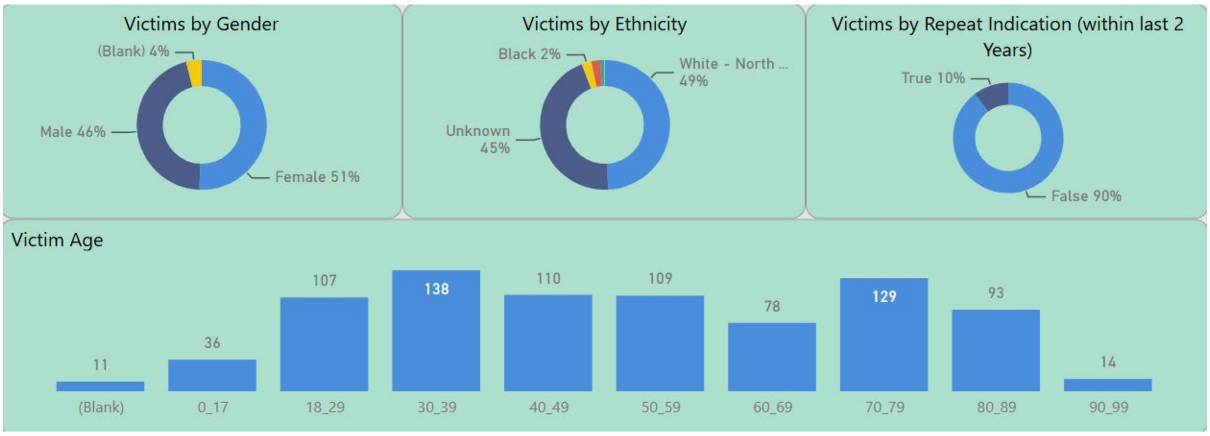
Metric Measured	1/7/21-30/6/22	1/7/22 - 30/6/23	1/7/23 – 30/6/24	01/07/24-30/06/25	01/07/25-30/06/26
Total Investigations	**594**	**940**	**1068**	**1477**	**1447**
Fraud Report Call for Service	**289**	**261**	**351**	**301**	**431**
Fraud Report NFIB Referral	**142**	**359**	**142**	**99**	**63**
Non-Crime Financial Investigation	**163**	**320**	**575**	**766**	**653**
Investigations with a Positive Outcome	**67**	**59**	**104**	**86**	**117**
Live investigations from that period	**28**	**38**	**154**	**62**	**225**
Number of fraud victims	**467**	**766**	**830**	**1146**	**1020**
Number of fraud suspects	**309**	**314**	**335**	**448**	**528**

The below chart plots the overall totals from table 1, above, for the period 1 July 2023 to 30 June 2026

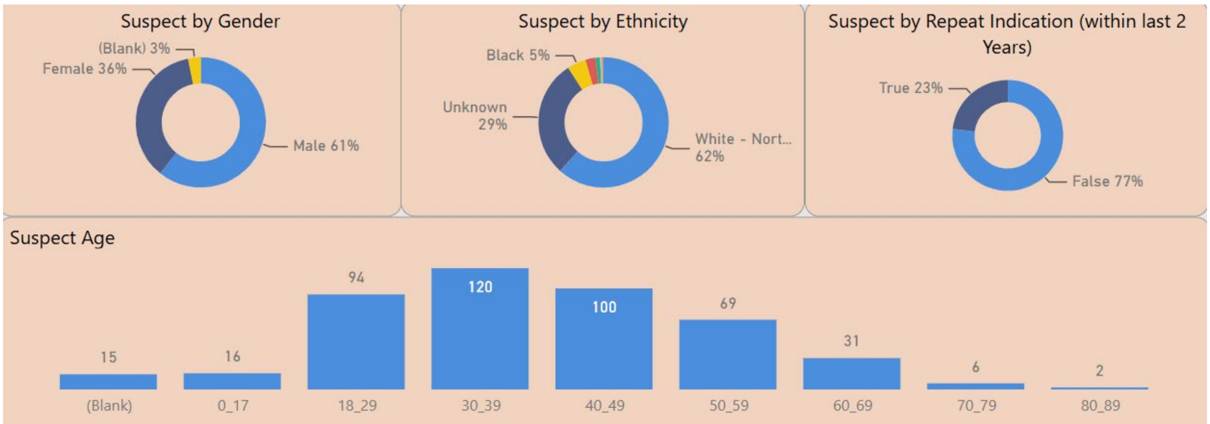
The below chart plots the total investigations for the current reporting period, 1 July 2025 to 30 June 2026, with a comparison against the previous 12-month period.



The below chart provides an analysis of fraud victims in Suffolk for the reporting period, 1 July 2025 to 30 June 2026



The below chart provides an analysis of fraud suspects in Suffolk for the reporting period, 1 July 2025 to 30 June 2026



The data presented shows continued changes in fraud demand, including increases in some categories. This provides scope to assess how best to address demand, including prevention.

3. APPROACH TO FRAUD INVESTIGATIONS – ROLE OF THE FRAUD ASSESSMENT UNIT (FAU)

3.1. The Fraud Assessment Unit (FAU) was formed in December 2021 with the aim to streamline, simplify and arrange the response to improve the service we provide to victims, in addition to providing further clarity for front line officers on fraud offences.

3.2. The FAU has a fraud strategic plan and is managed by the Workflow Management Detective Chief Inspector (DCI). The overarching aims are to reduce harm, loss and minimise risk to victims of fraud, building workforce capability, conducting quality fraud investigations and working together to counter fraud.

3.3. The team consists of a Detective Sergeant and three Detective Constables, and a Fraud Protect and Prevent Officer. All officers in the Fraud Assessment Unit enrol on a City of London Police Economic Crime Specialist Investigator Programme course (Note: this role was previously known as the Specialist Fraud Investigator course).

3.4. The key responsibilities of the FAU are: -

- Review all fraud investigations in Suffolk within 24 hours.
- Since October 2025, the FAU has conducted an initial four-week follow-up review of all Call for Service (CFS) and NFIB referral crimes.
- Review all closed fraud investigations within 48 hours of closure.
- Bespoke interview advice – suspect or victim.
- Bespoke investigative advice.
- Ongoing oversight with reviews of all live fraud investigations every 28 days
- Liaison with NFIB (National Fraud Intelligence Bureau) and Specialist Teams.
- Liaison with Serious Organised Crime (SOC) and the Eastern Region Special Operations Unit (ERSOU) and their Specialist Teams.
- Liaison with Trading Standards around bogus callers/rogue traders.
- Support local delivery of, and alignment with, the National Fraud Strategy.

3.5. The Constabulary's Fraud Unit has implemented a structured process whereby all fraud offences are routed through the FAU for initial evaluation. This approach ensures consistency and prioritisation in line with the Fraud Investigation Model (FIM) – a framework specifically designed to reflect the complex and evolving nature of fraud.

3.6. The FIM promotes a logical and methodical approach to fraud investigations, recognising that criminality, harm, and financial loss often continue beyond the point of reporting and into the investigative and data-gathering phases. A key principle of the model is the early identification and disruption of fraudulent activity, with a strong emphasis on limiting the duration of harm and preventing further victimisation.

3.7. Initial assessments conducted by the FAU focus on identifying opportunities for early intervention, securing evidence, and initiating protective measures. This proactive stance enhances investigative efficiency and victim safeguarding.

3.8. In addition to operational responsibilities, the FAU plays a vital role in capability development across the organisation. The team delivers targeted training to departments (including induction sessions for new officers) covering fraud recording protocols, investigative standards, and the Constabulary's strategic approach to tackling fraud.

3.9. Suffolk Constabulary records and investigates a wide range of fraud offences, many of which do not require direct intervention by the force. To ensure appropriate allocation of resources, the FAU plays a key role in identifying such cases prior to their entry into Athena, the crime recording system. The FAU provides frontline officers with guidance on the Report Fraud referral process, including the criteria for a 'Call for Service', which must be met for an offence to be formally recorded within Constabulary systems. This ensures that fraud cases are triaged effectively and routed to the most appropriate investigative pathway.

3.10. Suffolk Constabulary actively identifies potential money mules, individuals who facilitate the movement of illicit funds, through banking enquiries conducted by the FAU. Where individuals are found to have no prior offending history, the matter is addressed through the issuance of a 'cease and desist' notice, a recognised disruption tactic endorsed by the National Fraud Intelligence Bureau (NFIB). Alongside this, tailored crime prevention advice is provided, and any identified vulnerabilities are recorded and referred to the Multi-Agency Safeguarding Hub (MASH) for further support. This approach balances enforcement with safeguarding, aiming to prevent further exploitation while disrupting criminal networks.

3.11. The Fraud Protect and Prevent Officer post is now embedded within Suffolk Constabulary and plays a key role in delivering fraud prevention and protection initiatives.

4. APPROACH TO CYBER-ENABLED FRAUD AND SERIOUS ORGANISED CRIME

4.1. Suffolk Constabulary has established robust processes for the identification and mapping of Organised Crime Groups (OCGs). Coordination is managed through the Joint Suffolk & Norfolk Organised Crime Group Meeting (OCGM), in partnership with the Eastern Region Special Operations Unit (ERSOU), ensuring strategic oversight and alignment with regional priorities.

4.2. The Constabulary is actively focused on identifying OCGs involved in fraud through targeted tasking, intelligence development, and the work of the Cyber Specialist Capability Team. This team receives cyber fraud referrals from the National Fraud Intelligence Bureau (NFIB) and, through newly implemented processes, is expected to increase intelligence submissions and enable earlier preventative interventions.

4.3. Multi-agency collaboration is central to disrupting fraud linked to organised crime. Suffolk Constabulary works alongside partners such as the Department for Work and Pensions (DWP) and His Majesty's Revenue and Customs (HMRC) to deliver large-scale disruption of fraudulent activity, particularly where fraud is a secondary crime type.

4.4. Lead Responsible Officers (LROs) for OCGs within Suffolk Constabulary are briefed on nationally recognised disruption tactics, structured around the four strategic pillars – Prevent, Pursue, Protect and Prepare.

4.5. These officers have access to National Crime Agency (NCA) guidance on disruption tactics. Organised crime matters are regularly discussed at the Safer Stronger Communities Group (SSCG), a strategic partnership forum within Suffolk.

4.6. Suffolk and Norfolk Constabulary have a joint Cyber Crime Unit that forms part of the national Cyber Crime Unit. Nationally the role of Cyber unit is to work to the National Cyber Strategy (The UK National Cyber Strategy 2022). This is completed through National Led Regionally Managed Locally Delivered (NLRMLD) operating model set out by the National Police Chiefs Council (NPCC) and NCA.

4.7. The primary focus of the Cyber network is Computer Misuse Act offending, also known as pure cyber offending and linked offending. This includes but is not limited in scope to Denial of Service Attacks, Network Intrusion and Ransomware attacks. Linked offending covers offences such as payment diversion, stalking and harassment (assisting with victim protection and safeguarding), blackmail and account compromises.

4.8. This response is delivered across the 4 strategic pillars; the unit offers Pursue investigators trained in the tracking and tracing of cryptocurrency – supporting other departments and guiding on enquiries. The unit also includes Pursue investigators targeting Computer Misuse Act offences and linked offending, some of which overlaps with fraud and is categorised as cyber-enabled offending.

4.9. Through this Joint Suffolk and Norfolk Cyber Specialist Capability Team, the Constabulary supports national initiatives such as the Regional Cyber Resilience Centre and the Cyber Alarm Programme, contributing to strategic business engagement and preventative cyber security measures and supporting Regional Cyber Crime Units (RCCU's).

4.10. The Cyber Specialist Capability Team includes two embedded Cyber Security Advisers, who along with the rest of the team, provide tailored support to victims of cyber fraud—both individuals and businesses. The team has developed a bespoke system that generates personalised written advice for victims, aimed at reducing the risk of repeat victimisation and enhancing digital resilience.

4.11. The Specialist Crime and Intelligence Directorate, shared between Suffolk and Norfolk Constabularies, contributes additional resources within the Cyber Crime Unit, to the response against cyber-dependent fraud. This includes both reactive investigative capability and proactive work to prevent and protect the public from emerging threats.

5. ADDITIONAL POLICING CAPABILITY

5.1. Suffolk Constabulary maintains a pool of detectives within its Criminal Investigation Departments who have undertaken the foundation module of the Fraud Investigators Course, delivered by the City of London Fraud Academy. This training enhances their understanding of fraud typologies, investigative techniques, and evidential standards.

5.2. In addition, senior officers within the Constabulary have completed the Counter Fraud Managers Course, also hosted by the City of London Police, and are formally accredited as Fraud Managers. This ensures strategic oversight and informed decision-making in complex fraud investigations.

5.3. The Intelligence Directorate includes staff trained in the use of specialist systems to support intelligence development in financial and fraud-related investigations. These personnel are embedded within both area intelligence teams and the Joint Force Intelligence Team, with the number of trained staff continuing to grow, reflecting a commitment to expanding analytical capability.

5.4. Suffolk Constabulary has continued to support Operation Henhouse, a national enforcement initiative involving the National Crime Agency, the National Economic Crime Centre and City of London Police. During the February 2026 deployment, the operation resulted in six voluntary interviews and the progression of 27 fraud investigations.

6. SUPPORTING VICTIMS

6.1. Fraud investigations are recorded in the same way as other investigations, using an investigation plan to ensure compliance with the Victims' Code of Practice (VCOP). This applies to all Suffolk fraud investigations.

6.2. Suffolk Constabulary's Fraud Assessment Unit (FAU) is engaged with Report Fraud Victim Services, which is a team within the National Fraud Intelligence Bureau (NFIB). Report Fraud Victim Services provides a three-tiered support system for victims of fraud and cybercrime across police forces in England and Wales:

- Level 1: Victim Contact which gives appropriate support to less complex cases (non-vulnerable victims.) Support typically includes protective advice, referrals to local services, and general guidance to help prevent re-victimisation.

- Level 2: Victim Care handles more complex and difficult cases (based around an assessment of vulnerability of the victim). Support is more intensive and may involve multi-agency coordination, including referrals to the NHS, Social Services, and other specialist support networks.

- Level 3: Where serious risks of harm arise following contact with victims whereby a police force response may be required. This local level support focuses on safeguarding and supporting the most vulnerable at-risk individuals, using a multi-agency approach and/or to manage other issues identified through level 1 and/or level 2 contact. Level 3 victims are referred as a Vulnerable Person Alert (VPA) to the Constabulary via the Foundry portal.

6.3. There is a process in place for level 1 and 2 victims to receive support from the RFVS. If RFVS has concerns, it refers the matter to the Constabulary's Fraud Assessment Unit. This may result in a visit by an officer, contact from the FAU and/or involvement from the Fraud Protect and Prevent Officer.

6.4. In many instances, victims will have already engaged with Report Fraud prior to any contact with Suffolk Constabulary. During their initial interaction, they are typically provided with safeguarding advice and information on preventative measures to help mitigate further risk.

6.5. Suffolk Constabulary publishes information on its website providing clear guidance and advice to the public, together with links to Report Fraud, CIFAS (Fraud Prevention), the Financial Conduct Authority, Financial Ombudsman and Trading Standards.

6.6. Staff within the Crime Co-ordination Centre (CCC), Contact and Control Room (CCR) and Fraud Investigators provide information and guidance to victims. An additional process has been adopted within the CCC to enable victims to receive an email with crime prevention guidance.

6.7. Where relevant, Constabulary staff complete vulnerable person referrals for multi-agency assessment. These are processed by the Multi-Agency Safeguarding Hub (MASH) who can make determinations about how best to safeguard a potentially vulnerable person, sharing information with other partner agencies where relevant to best safeguard that person.

6.8. Suffolk Constabulary complies with the national protocol of updating victims when an investigation is recorded locally after an NFIB referral. The recording officer is responsible for contacting the victim, agreeing the level of contact and ensuring they are aware of the transfer of responsibility to a Suffolk Investigator.

7. POLICING IMPROVEMENT

7.1. Since the publication of the National Fraud Strategy 2026-2029 the national direction for tackling fraud has been reframed around three pillars: Disrupt, Safeguard and Respond. The Strategy places emphasis on earlier disruption of fraud enablers, improved victim support, stronger intelligence sharing, enhanced law enforcement capability and a more proactive approach to protecting individuals and businesses from fraud.

7.2. Key national developments relevant to Suffolk Constabulary include the continued operation of Report Fraud, the development of Report Fraud Victim Services, the creation of the Online Crime Centre, greater use of data-led PROTECT activity, improved coordination across law enforcement and industry, and the planned introduction of a Fraud Victims Charter in 2027.

7.3. Suffolk Constabulary's local activity aligns with these priorities through the work of the Fraud Assessment Unit, victim safeguarding arrangements, fraud prevention activity, partnership working with Trading Standards and regional/national partners, and continued development of fraud investigation capability.

8. PARTNERSHIP WORKING

8.1. Suffolk Constabulary is represented at regional fraud and economic crime delivery groups, which seeks to share best practice. This will continue with any areas of best practice being considered for adoption within Suffolk.

8.2. Part of the Constabulary engagement in the regional meetings is to undertake a quarterly assessment of our position against our force and regional level strategy and action plan, using the model of the 4 P's – pursue, protect, prevent, and prepare.

8.3. The Constabulary already works with several key partners in relation to fraud including the Eastern Region Specialist Operations Unit, National Crime Agency, and City of London Police. In addition, Suffolk Constabulary works collaboratively with colleagues in Norfolk Constabulary to share best practice and access shared resources within Protective Services. There is regular dialogue between Fraud Investigators in Suffolk and staff within the Joint Suffolk & Norfolk Cyber Unit due to interconnectivity between many fraud offences and cyber-crime.

8.4. Suffolk Constabulary supports a multi-agency approach to tackling fraud and is seeking to further good working relationships with Suffolk Trading Standards, and the Multi-Agency Safeguarding Hub (MASH).

8.5. In June 2026, Suffolk Constabulary, Suffolk Trading Standards and Cyber Security Advisors launched Suffolk Against Fraud (SAF). The initiative brings together organisations and businesses across Suffolk to support a consistent countywide approach to preventing and tackling fraud, strengthening local partnership arrangements and improving coordination of fraud prevention activity.

9. ANTICIPATED DEVELOPMENTS FOR THE NEXT REPORTING PERIOD

9.1. A new 'Fraud and Economic Crime App' is now available, designed and developed by the City of London Police Fraud Operations Team and the Economic and Cyber Crime Academy.

9.2. The App will support all frontline officers and staff not ordinarily exposed to fraud and economic crime, ensuring they can give the very best response when serving the public and preventing repeat victimisation. It provides a quick-access 'go-to' guide on topics such as: -

- When and how to report a fraud or economic crime;
- Legislation: a quick reference to the right legislation to use at the right time;
- Providing the best advice for protecting the public from fraud;
- Victim care: principles to apply and managing ongoing support; and
- How to deal with cash seizures and early considerations during an investigation.

9.3. At present the Constabulary ICT Governance and Support is not in place to launch the Fraud App. A project is underway to provide this governance and support.

9.4. The Constabulary will continue to monitor the benefits of Report Fraud, particularly in relation to improved intelligence packages, victim contact and alignment with the National Policing Strategy for Fraud, Economic and Cyber Crime 2023-2028.

9.5. The College of Policing has introduced two fraud-related NCALT training packages to assist CCR staff and frontline officers when dealing with fraud reports made to the Constabulary. These training packages include guidance on Call-For-Service criteria and when a report should be made to Report Fraud. The Constabulary will make these training packages mandatory for all relevant staff once they are available through the Learning Management System (LMS) portal from September 2026.

10. FINANCIAL IMPLICATIONS

10.1. To support improvement in many of the areas outlined, continued investment in training and people to fulfil key functions will be required.

11. OTHER IMPLICATIONS AND RISKS

11.1. The data presented shows a general increase in reported cases of fraud which is consistent with the national picture. This gives us scope to assess how best to address the rising demand, including prevention.

11.2. It is recognised that fraud is under reported to both Report Fraud and policing, therefore the true scale of this type of criminality and its impact within Suffolk and nationally is unknown.

11.3. The nature of fraud has changed over time and continues to develop, and those committing fraud on a larger scale seek new ways of offending, particularly online and through use of Artificial Intelligence (AI).

11.4. Suffolk Constabulary has a small number of dedicated fraud staff by comparison to other police forces within the Eastern Region.

11.5. The Constabulary has seen little improvement in the ability to demonstrate proactive identification of organised crime groups where the primary criminality is fraud, use of ancillary orders in connection with fraudsters or co-ordinated prevent activity in relation to organised fraud criminality.

12. OPPORTUNITIES

12.1. There are opportunities that are starting to be realised to progress a multi-agency approach to fraud investigation and prevention. Further connectivity between agencies is intended to lead to consistent approaches to victim support, coherent and aligned messaging and a reduction in duplication with more complete assessments of fraud through information sharing.

12.2. The Eastern Region Specialist Operations Unit are investing in additional capabilities within the area of economic crime and cyber-enabled crime.

13. CHIEF OFFICER CONCLUSION

13.1. Suffolk Constabulary continues to strengthen its response to fraud – in line with national priorities and our Police and Crime Plan. This report outlines how the force is improving prevention, investigation, and victim support in line with the new National Fraud Strategy *Disrupt, Safeguard and Respond* pillars.

13.2. Our dedicated Fraud Assessment Unit reviews every fraud case at an early stage, to ensure investigations are prioritised, victims safeguarded and opportunities for early disruption identified. The Constabulary continues to build its specialist capability through accredited training, expanded partnership work with the National Crime Agency, Eastern Region Special Operations Unit, Trading Standards, Joint Cyber Unit, and through introduction of a Fraud Protect & Prevent Officer to support community education and crime prevention.

13.3. Victim care remains a key focus, with tiered support now provided through the national Report Fraud Victim Services and local multi-agency safeguarding for the most vulnerable. There is an enduring focus on crime prevention.

13.4. This report acknowledges several challenges, including a sustained increase in Fraud demand, which encompasses growing investigative complexity against the backdrop of a comparatively small specialist fraud team. Investigations become increasingly complex through the evolving nature of cyber-enabled and AI-driven offending which continues to place acute pressure on resources. However, the Constabulary is working to address these challenges through improved processes, capability development, and investment in new technologies, including a forthcoming national fraud app for frontline officers.