SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Purpose

To provide an overview of Scottish Police Authority ('the Authority') oversight of cybercrime.

Authority Oversight

The Authority's oversight of Police Scotland's efforts to tackle cybercrime is led by the Authority's Policing Performance Committee and reported publicly to the Authority's Board Meetings.

An overview of key work in progress to address cybercrime in Scotland, and the Authority oversight of this, is summarised below.

1. 2030 Vision

1.1 Police Scotland's 2030 Vision was launched in September 2024. This has four areas of focus:

- **Safer Communities**
- **Less Crime**
- **Supported Victims**
- **A thriving workforce**

1.2 The Vision includes a commitment to 'establish a cyber and fraud specialist division to enhance our response in Scotland' and 'develop our capability through cyber and online training for the workforce, ensuring support and guidance for officers and staff'.

1.3 Police Scotland reported to the Policing Performance Committee in December 2025 that the Cyber and Fraud Unit had been established by Police Scotland and will continue to evolve to meet demand.

1.4 Police Scotland also reported that Full Business Case to support joining the Fraud Cybercrime Reporting and Analysis Service (FCRAS), led by the City of London Police, is in development and is expected to be presented to the Authority for consideration in the 2026-27 financial year.

2. Policing in a Digital World

2.1 The Policing in a Digital World Programme was established in 2023 to equip Police Scotland to respond to cybercrime through the '4Ps Approach': Pursue, Protect, Prepare and Prevent.

2.2 The Authority has had regular oversight of the programme since it was established. During consideration of the most recent update presented in March 2025, Members' scrutiny focused on understanding how good local practice was rolled out on a national basis, and that appropriate training to support cybercrime was rolled out across the organisation for officers and staff to support the investigation of cybercrime.

2.3 Members have taken assurance from key developments in the Policing in a Digital World Programme, for example:

- **Child Abuse Image Database and Facial Matching (CAID FM):** The introduction of this capability has brought about efficiencies through the use of Artificial Intelligence to automate the review of images. A case with 10,000 images would typically an officer up to three days to review. Utilising the CAID FM capability, a case of a similar size can be reviewed in an hour. This has helped shift the balance from reviewing images to identifying victims, with the overarching aim of safeguarding children.
- **Digital Forensic Vans** are used to examine digital devices to increase the likelihood of identifying investigative lines of enquiry at locus, while reducing delays in the owner being deprived of their device(s) for extended periods of time for the purpose of examination. This provision not only meets the milestone set out in the 2030 Vision for enhanced capabilities of digital forensic laboratories to create efficiencies, it also contributes to other milestones with regards to an enhanced service to the communities and welfare for Police Scotland staff.
- **Police Cyber Alarm (PCA):** As part of Police Scotland's Cyber Protect activities in line with the milestones set out in the 2030 Vision, PCA was launched across Scotland in August 2024 for use by businesses and organisations to monitor threats and receive regular vulnerability reports. As of 7th February 2025, 98 organisations have signed up to utilise the PCA capability.

3. Quarterly Performance and Understanding Cybercrime

3.1 From April 2025, Police Scotland introduced a performance indicator to report the number of cybercrimes in their public performance report to PPC. This indicator monitors all crimes that have a cyber 'tag' applied to them by an officer. As with any new crime tag, it will take time to embed the practice with front-line officers to mark a crime where a cyber element is present.

3.2 The cyber tag should be used when the following circumstances are involved in the crime: the commission or attempted commission of traditional crimes such as theft, fraud, extortion, threats etc. using

the internet, or by otherwise accessing a computer system, device or network.

3.3 Cyber-enabled crimes are instances where technology has been used to enhance another crime or as a means to commit a crime. Cyber-enabled crimes can be found across all crime groups and include, but are not limited to:

- Abuse via social media;
- Threats via email;
- Online fraud and other economic crime;
- Theft from online bank account;
- Sexual exploitation and sextortion;
- Grooming and offences against children as included in the Sexual Offences (Scotland) Act 2009;
- Stalking.

3.4 Cyber-dependent crime is when a commission or an attempted commission of crime in order to compromise a computer device, network or system, where the devices are both the tool for committing the crime and the target of the crime. These crimes can include, but are not limited to:

- Creating, selling/distributing, or deploying Computer Viruses, Malware or Trojans with nefarious intent;
- Attacking or impairing the normal use of a website – Denial of Service attacks (DoS);
- Hacking / network intrusion / account takeover or any other unauthorised access of ICT;
- Corrupting / controlling a system via email or other means.

3.5 The table below shows the number of crimes that have had a cyber tag applied to them over the first two quarters of this reporting year. As this is a new metric trend information is not yet available and will be developed over time, with the volume of these types of crime expected to increase as the use of the cyber tag embeds.

Table – Crimes with a Cyber tag	**Number of cyber-crimes**
2025-26 Q1 YTD	2,812
2025-26 Q2 YTD	5,712

3.6 However, the Authority believes it is important to look beyond this figure when discussing the widespread nature of cyber-enabled and cyber-dependent crime as described above.

3.7 The Authority therefore considers crimes that have a cyber element which are already reported, but have not yet had a cyber tag applied due to the emerging practice described above. Examples are provided in the table below.

Table – Crimes that are mostly Cyber/Digitally Enabled	**Online Child Sexual Abuse**	**Fraud**
2024-25	1,989	15,253
Five-Year Mean	1,943	14,552
% Change	+2.4%	+4.8%

3.8 In reference to the above example of fraud, while the Scottish Government's Recorded Crime analysis estimates that 59% of all fraud crimes in 2023-24 were cyber-enabled, the National Crime Agency estimate for the whole of the UK is higher, at 67%.

3.9 It can be reasonably assumed that, due to the nature and use of every-day technology such as mobile phone and social media, that crimes which are thought as 'traditional crimes' will have a cyber-enabled element or digital footprint. This could include Domestic Abuse, Sexual Assault (understanding the relationship between perpetrator and victim), Stalking, Hate Crime, Cyber-Bullying etc. For example, the Scottish Government Recorded Crime analysis estimates that 30% of all sexual crimes in 2023-24 were cyber-enabled.

3.10 As an example in January 2020, Refuge, the UK's largest domestic violence charity stated that in 2019, 72% of service users experience abuse through technology. According to Police Scotland data, in 2024-25 there were 39,323 Domestic Abuse Crimes recorded.

4. Digital Forensics

4.1 Digital Forensics are crucial to modern policing. It provides the capability to identify, extract and present digital evidence that is often integral to investigations, and is also required to keep people safe across Scotland. Due to the increase in cyber related crimes, there is a backlog of cases awaiting digital examination.

4.2 Both the Authority and Police Scotland maintain that a sustainable Digital Forensic capability is integral to evidential integrity in the criminal justice process.

4.3 Furthermore, the approach reflects the ambitions of the Scottish Government's Digital Strategy by embedding innovation, resilience, and public trust into how critical digital services are delivered across Scotland's justice system.

4.4 The Authority has received several updates from Police Scotland on its approach to digital forensics and will continue seek assurance on the embedding of this approach.

5. Conclusion

5.1 A conclusion can be drawn that the demand on Police Scotland to investigate crime that is increasingly complex due to a cyber or digital component is greater than ever. Therefore, the number of crimes that have had the cyber tag applied in Q1 and Q2 of this year is not reflective of the scale of crimes that have a cyber element.

5.2 The Authority takes assurance from Police Scotland's implementation of a cyber tag for crime with a cyber-enabled or dependent component however, the Authority wishes to see embedded practice that ensures this tag is used on all crimes which are cyber-enabled.

5.3 Through this change in practice, there will be an improved understanding of the scale and complexity of crime involving a cyber element. This will inform the Authority's assurance and oversight of how Police Scotland plans to adapt to address this demand. Police Scotland will require to direct resources in order to continue to investigate growing cyber-enabled and cyber-dependent crime.