SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Audit, Risk and Assurance Committee
13 August 2026

Item 9.3: Police Scotland Annual Data Loss, Fraud and Theft Report
Presenter: ACC Lynn Ratcliff, Professionalism and Assurance
Appendix: Appendix A: Data Loss Incidents

Purpose

To provide members with information about theft, fraud and data loss incidents occurring within Police Scotland during 01 April 2025 to 31 March 2026 and provide an assurance statement as to the reporting process.

Recommendation

For Discussion

Strategic Alignment

Strategic outcome(s)	Police Scotland Strategic Outcomes 1, 2, 3, 4 and 5: 1.Threats to public safety and wellbeing are resolved by a responsive police service 2.The needs of local communities are addressed through effective service delivery 3.Public and communities are engaged, involved and have confidence in policing 4.Our people are supported through a positive working environment enabling them to serve the public 5.Police Scotland is sustainable, adaptable and prepared for future challenges
Risk alignment	Police Scotland DP and Infosec Risks
Prior governance	ACC Professionalism and Assurance, CDIO
Stakeholder engagement	Stakeholder engagement takes place when regulatory reporting requirements are engaged and notifications required for impacted individuals. A collaborative approach is required with DPO providing guidance to internal

	stakeholders, informing of the content and style of notifications to individuals.
Rationale for taking in private	• This paper is presented in line with SPA Corporate Governance Framework Standing Orders Section 21(d) where matters to be discussed are the subject of legal proceedings (including misconduct or disciplinary proceedings) or where the information to be discussed consists of or includes legal advice provided to the SPA or to a third party. • This paper highlights controls in place to prevent theft and fraud and investigations into data loss. • Discussion in public is likely to inhibit the free and frank provision of advice or the free and frank exchange of views for the purpose of deliberation.

Implications

Community		Data & Privacy	✓	Environmental	
Equalities & Human Rights		Financial		Health, Safety & Wellbeing	
Legal	✓	Workforce			

1 Report Detail

1.1 Background

1.2 As highlighted in the Scottish Police Authority Governance and Accountability Framework document, the SPA is required to ensure that adequate systems of internal control are maintained by the Authority, including effective measures against fraud and theft, consistent with the Fraud section of the Scottish Public Finance Manual (SPFM). Significant lapses of data security should also be reported.

1.3 The SPFM further defines that Fraud can be perpetrated by persons outside as well as inside an organisation and by collusion. The term "fraud" is commonly used to describe a wide variety of dishonest behaviour such as deception, forgery, false representation, and concealment of material facts. It is usually used to describe the act of depriving a person of something by deceit, which may involve the misuse of funds or other resources, or the supply of false information.

1.4 Further detail

1.5 The following instances of Theft and Fraud have occurred within Police Scotland and the SPA during the 2025/26 financial year (01 April 2025 to 31 March 2026):

Incident	Circumstances	Value
Fraud	A member of Police Staff omitted information within their vetting forms and obtained employment within Police Scotland.	£64,208

1.6 A check has been carried out with the Professional Standards Department who have responsibility to manage any investigations into incidents of organisational related fraud and theft and who receive information from a wide range of sources.

1.7 Data Loss Incidents

1.8 Within Police Scotland there have been 386 incidents of data loss reported during 2025/2026. All incidents have been investigated and risk assessed to establish if they meet the threshold for reporting to the Information Commissioner Office (ICO).

1.9 Accordingly, there have been 9 incidents of data loss (personal data breach) reported to the ICO within the period.

1.10 The Committee should be assured that when incidents are identified, each incident is reviewed, and the appropriate mitigating action(s)

taken to reduce the risk to the organisation of such losses. The actions taken focus on:

- Being appropriate to the data loss involved; and
- Are in line with the actions the organisation would be expected to
- take and involve future safeguarding of assets; and
- Mitigating the risk of such losses occurring again in the future

1.11 Members may wish to note that since the implementation of UK GDPR the reporting process to the Information Commissioner's Office (ICO) has changed. The reporting of data loss incidents to this committee has been updated to reflect these changes.

1.12 The main areas of change when managing and/or reporting data loss incidents are as follows:

- Organisations have 72 hours from the time they are made aware of the data loss to gather information and carry out an assessment.
- Each incident should assess the potential impact and severity on the individuals affected against their rights and freedoms. This assessment will also influence the decision to report to the ICO or subjects affected.
- Notification to the ICO is only triggered where a breach is likely to result in a risk to the rights and freedoms of an individual.
- Communication of a breach to the individual is only triggered where there is a high risk to their rights and freedoms.

1.13 Reported Data Loss Incidents

1.14 Where a data loss incident has occurred and meets the threshold for reporting to the ICO, the following details will be provided to the members and are included within Appendix 'A' of this report:

- Risk level
- Circumstances
- Details of investigation carried out
- Mitigation
- Criteria for reporting
- Organisational learning
- ICO response

2 Strategic alignment detail

2.1 Strategic alignment to strategic police plan and other key enabling strategies

Strategic outcome(s)	All five policing strategic outcomes are applicable.

2.2 Alignment to risk register and risk appetite

Risk alignment	Police Scotland DP and Infosec Risks

2.3 Prior governance

Prior governance	ACC Professionalism and Assurance, CDIO

2.4 Stakeholder engagement

Stakeholder engagement	Stakeholder engagement takes place when regulatory reporting requirements are engaged and notifications required for impacted individuals. A collaborative approach is required with DPO providing guidance to internal stakeholders, informing of the content and style of notifications to individuals.

3 Implications detail

Community		Data & Privacy	✓	Environmental	
Equalities & Human Rights		Financial		Health, Safety & Wellbeing	
Legal	✓	Workforce			

3.1 The report concerns data loss incidents and personal data breaches. Incidents have been investigated and risk assessed, with ICO reporting and mitigation undertaken where required.

3.2 There are legal implications arising from this report. The paper relates to theft, fraud and data loss incidents, including personal data breaches, and therefore engages legal duties under UK GDPR and the DPA 2018. Incidents have been assessed against the relevant reporting thresholds, with notification to the Information Commission and/or affected individuals undertaken where required. Some matters may also give rise to employment, misconduct, disciplinary or other legal proceedings, which supports consideration of the paper in private session where appropriate.

Table 1: Number of reports of Data Loss Incidents received 2025/2026

	Q1	Q2	Q3	Q4	TOTAL
Incidents reported to the ICO	2	1	4	2	9
Incidents not meeting criteria to report to ICO	110	90	90	96	386

Table 2: Number of reports of Data Loss Incidents received 2024/2025

	Q1	Q2	Q3	Q4	TOTAL
Incidents reported to the ICO	0	0	2	1	3
Incidents not meeting criteria to report to ICO	127	103	118	125	473

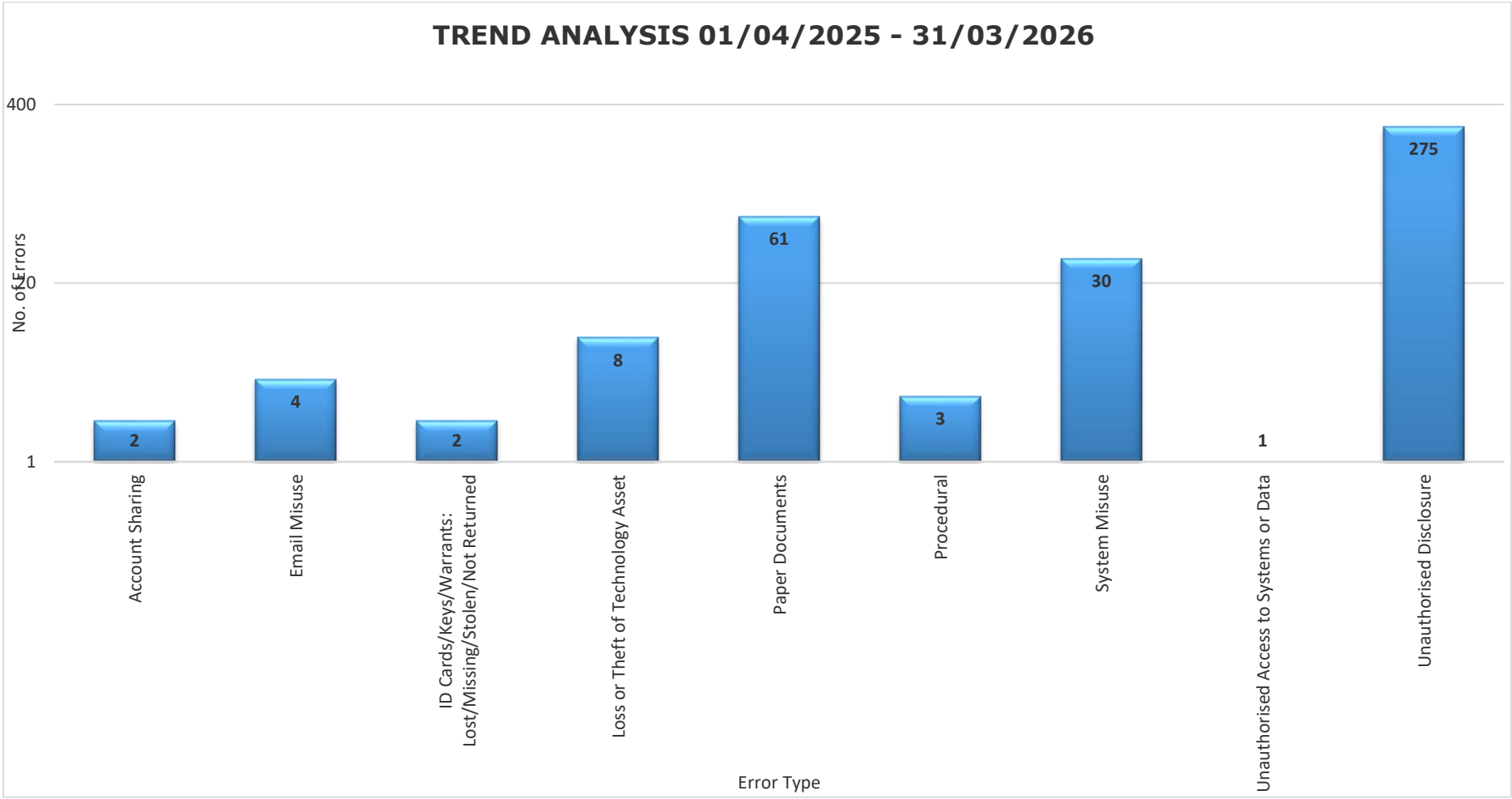
Table 3: Number of reports of Data Loss Incidents received 2023/2024

	Q1	Q2	Q3	Q4	TOTAL
Incidents reported to the ICO	0	0	1	0	1
Incidents not meeting criteria to report to ICO	95	142	81	143	461

Appendix A

Table 4: Details of Incidents Reported to ICO during 01 April 2025 to 31 March 2026

Date of Incident	Incident Number	Incident Type	Details of Incident	Action Taken & Mitigation Measures
26/04/25	25-0363	Unauthorised Disclosure	Address of victim disclosed within a Custody Report.	Safeguarding measures put in place Advice and guidance DPO reported to ICO - NFA
09/06/25	25-0492	Unauthorised Disclosure	Use of Google translate	Improvement Action Probationer Governance review Additional support measures DPO reported to ICO - NFA
10/06/25	25-0794	Unauthorised Disclosure	Unlawful access of police systems Officer suspended.	DPO reported to ICO
15/10/25	25-0882	Loss or Theft of Technology Assets	Lost laptop notification and notes relative to Investigation Device stunned. Management provided that there are no risks identified from the loss.	Advice and guidance provided DPO reported to ICO – NFA
08/05/25	25-0943	Loss or Theft of Technology Assets	PSoS production disc reported lost during delivery to the PFs office (Criminal Case). After thorough investigation and a full search there is no trace of the disc.	Logistical error – advice and guidance. DPO reported to ICO – Recommendations received NFA
14/11/25	25-0994	Unauthorised Disclosure	Incorrect attachments relating to ill health retirement attached to an email and sent to an incorrect recipient.	The email and attachment has been fully deleted. Person whose information was shared has been made aware. DPO reported to ICO Recommendations received NFA

11/06/25	25-1051	Unauthorised Disclosure	National Case update – 20% of Flat numbers did not pull across – risk that communication may not be delivered correctly.	No harm identified COPFS review DPO reported to ICO - NFA
23/01/26	26-0071	Unauthorised Disclosure	Witness details provided to accused in error	No risks to witnesses identified Paperwork recovered Corrective advice DPO reported to ICO - NFA
10/02/26	26-0114	Paper Documents	Custody hospital record left in public waiting area. NHS staff discovered paperwork and contacted Police.	Paperwork retrieved Data subject notified DPO reported to ICO - advice provided and case closed

Data Loss Incidents