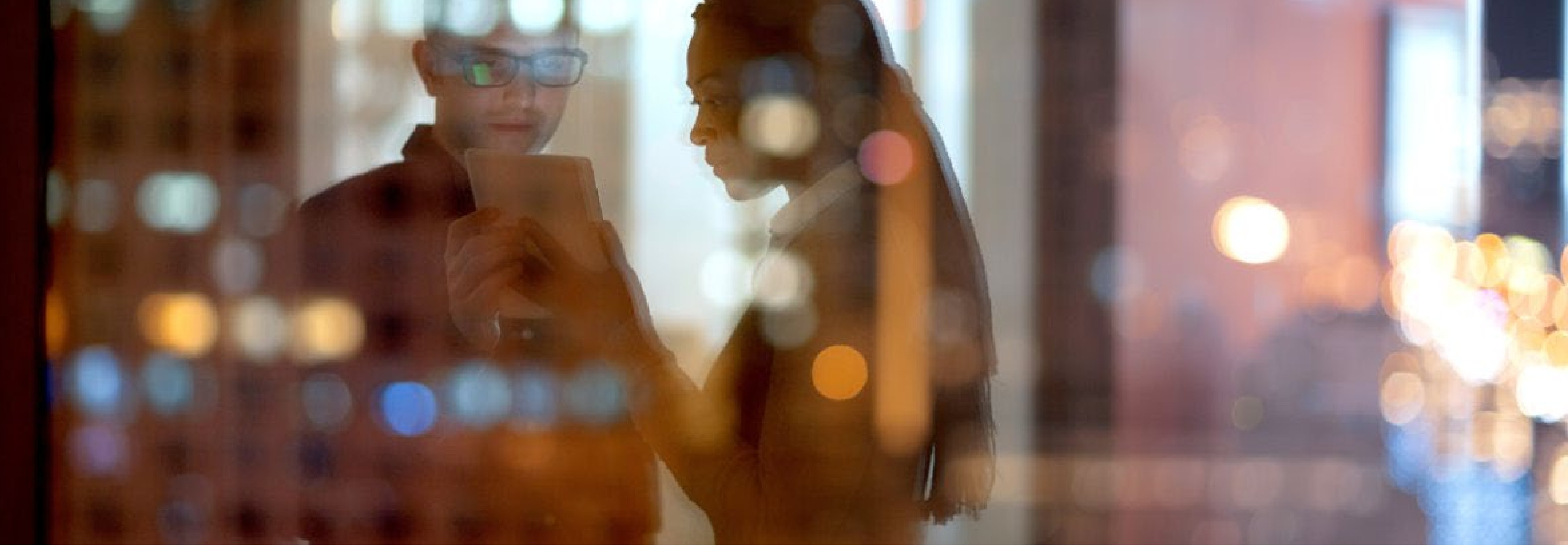

Information Commissioner’s Office

Internal Audit Report: Fines Recovery

September 2021

mazars

Contents

Disclaimer

This report ("Report") was prepared by Mazars LLP at the request of the Information Commissioners Office (ICO) and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit the ICO and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1of this report for further information about responsibilities, limitations and confidentiality.

mazars

01 Introduction

As part of the agreed Internal Audit Plan for 2021/22, we have undertaken a review of the Information Commissioner's Office (ICO) arrangements for the recovery of fines. We have reviewed key controls to assess whether the ICO's framework and processes are designed and operating effectively. This included the following risk areas:

- Policies and procedures;
- Roles and responsibilities;
- Fines issued;
- Debt recovery of fines;
- Monitoring and reporting;

Full details of the risks covered are included in **Appendix A1**.

The audit covered fines issued by the ICO in respect of non-payment of annual fees and where breaches of legislation that ICO regulates have occurred.

The 'Fees and Income' audit (September 2020) gave coverage to the identification of organisations that have not complied with legislation or payment of annual fees. This audit will focus on the process from the point of the fine being issued.

We are grateful to the Director of Investigations, Director of Digital, IT and Business Services and other staff for their assistance during the audit.

The fieldwork for this audit was completed whilst government measures were in place in response to the coronavirus pandemic (Covid-19). Whilst we completed this audit remotely, we have been able to obtain all relevant documentation and/or review evidence via screen sharing functionality to enable us to complete the work.

This report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Any such matters have been discussed with the relevant staff.

02 Background

Financial Recovery Unit: Fines issued in respect of non-compliance with ICO regulated legislation

The ICO has both investigative powers and regulatory powers, which include taking enforcement action under the Data Protection Act (DPA) 2018 (and DPA 1998) and Freedom of Information Act 2000 (FOIA).

Where breaches have been found to have occurred, the Financial Recovery Unit (FRU) is tasked with the management and recovery of Civil Monetary Penalties (CMP) issued for breaches of regulated legislation.

The ICO has the power to issue monetary penalty notices for serious contraventions of GDPR of up to 4% of an organisations global turnover, whilst breaches of Privacy and Electronic Communications Regulations (PECR) can result in fines of up to £500,000 being issued.

If a CMP is issued to an organisation, they have 28 days to make the payment or make an appeal to the First-tier Information Rights Tribunal. The organisation is also able to request a payment plan. If payment has not been received or an appeal made to the Tribunal, two further letters will be sent to attempt to recover the fine before alternative methods of enforcement are utilised, e.g. referral to an external litigation and recovery agency which assists with debt recovery.

Another common scenario in the recovery of fines is where the organisation responsible for the breach will put itself into liquidation. In these instances, ICO utilises its creditors rights and can apply to remove the liquidator chosen by the Director of the organisations and appoint one of its own preferred insolvency practitioners in order to recover the fine amount owed.

The status of all fines is monitored through a Case Management System; Crimson.

The FRU monitors performance on its recoveries through the Management Dashboard which is reported to management on a weekly basis. This provides information on existing payment plans (amounts paid and outstanding) and the status of recovery actions where Insolvency Practitioners have been appointed.

A spreadsheet named the Civil Monetary Penalty Register is maintained and records all fines issued by FRU and the amounts paid/recovered to date. The information is provided quarterly to the ICO Finance Department who subsequently report this to the Department of Digital, Culture, Media and Sport (DCMS) and HM Treasury.

In reporting for Q4 2020/21, FRU reported that £11,766,900 of £41,959,000 (28%) fines issued had been recovered during the financial year 2020/21.

Fines issued in respect of non-payment of Data Protection Fees

All organisations and sole traders that process personal information must pay a Data Protection ('DP') fee to the ICO unless they are exempt. The fee is payable on an annual basis.

Reminders are sent six weeks and three weeks before the expiry date of each registration by the Payments and Penalties Team.

Once the registration has lapsed, checks are undertaken to confirm whether the organisation is still trading. Once it has been confirmed that the organisation is still trading, 21 days from the date of registration expiring, a NOI letter is issued providing 21 days to either make payment of the registration fee or make representations as to why the payment has not been made.

If no response is received, a Final Penalty Notice ('FPN') letter is issued which provides a further 28 days to make the payment or lodge an appeal to the Tribunal. The FPN letter advises the organisation that as they have not responded to previous correspondence including the NOI, they will be subject to a fine as well as still having to pay the relevant data protection fee.

The fine amount is dependent on the Tier group that the organisations sits within:

- Tier 1 - Fine £400 plus £40 registration fee (£440)
- Tier 2 - Fine £600 plus £60 registration fee (£660)
- Tier 3 - Fine £4,000 plus £2,900 registration fee (£6,900)

Payment plans are available but only for the fine amount. The DP fee element of any FPN is to be paid in full and does not form any part of a payment plan. Payment plans for amounts less than £5,000 must be authorised by the Team Manager, whilst those exceeding £5,000 must receive authorisation from the Group Manager.

Fines which remain unpaid are transferred to external debt recovery agency, Forbes.

In light of the Covid-19 pandemic, the decision was taken by senior management in March 2020 to suspend the collection of overdue payments in respect of the DP fee so as not to burden organisations already experiencing financial and capacity pressures. A page was set up on the ICO website with a statement from the Commissioner setting out the ICO's regulatory approach during the pandemic, which did not explicitly state that collection of these fees were suspended but that the ICO would "*be flexible in our approach, taking into account the impact of the potential economic or resource burden our actions could place on organisations.*"

The collection processes resumed on 7 May 2021.

The status of NOIs and FPN's are monitored by the Payments and Penalties Team daily through reports issued by the Business Development team. Analysis of the figures is undertaken on a weekly basis and reported to the Director of Digital, IT and Business Services and Head of Business Services via email.

The Group Manager and Team Manager met with Forbes in July 2021 to discuss how to proceed with aged debts from prior to March 2020. The Payments and Penalties Team completed a review of the aged debts in August 2021 to confirm whether the organisations are still trading or have made payments in the intervening time, in order to make recommendation as to whether to proceed with enforcement action. A final decision on the approach to take (e.g. whether to provide a final opportunity to pay, given the gap of at least 18-months since the last contact) is expected to be made at the next meeting in September 2021.

Reporting from the week ending 20 August 2021 stated that since collection processes resumed, 2,335 NOIs have been issued, of which 1,283 (54.95%) have been paid before the deadline. In this period, 75 FPNs have been issued with 16 full payments of both the DP fee and the fine being collected and 20 payments of the DP fee only.

03 Key Findings

Assurance on effectiveness of internal controls

Substantial Assurance

Rationale

The internal audit work carried out has provided **Substantial Assurance**. Please see Appendix A1 for the detailed scope and definitions of the assurance ratings.

Our audit has concluded that there is a generally sound control framework in place, however our work has identified one housekeeping recommendation at **Section 04**.

Number of recommendations

Priority 1	Priority 2	Priority 3	**Total**
-	-	**1**	**1**

3.1 Examples of areas where controls are operating reliably

Non-compliance with ICO regulated legislation

- We confirmed that the ICO has policies and procedures documented for its processes related to fines issued in respect of non-compliance with ICO regulated legislation. We reviewed these and confirmed that they are adequate in setting out the procedures, roles and responsibilities and had been reviewed within the past two years, with the exception of one document, which was dated November 2018. We have made a Priority 3 recommendation with regard to this at Section 04.
- We received a list of all fines issued in respect of breaches of legislation regulated by the ICO and reviewed a sample of ten. Our testing confirmed in all instances that:
  - A Notice of Intent had been correctly issued following investigation.
  - A Monetary Penalty Notice had been issued, where payment had not been received within 28 days;
  - Where a payment plan had been agreed, payments had been monitored and made at the expected intervals;
  - Where fines were being appealed or further activity was required to recover the fine (e.g. securing 'Consent to Act' and appointing a preferred liquidator where a company has been placed in.to liquidation by its Director), evidence was available to demonstrate the action taken.
- We reviewed a sample of aged debts within the Crimson case management system to confirm that there had been consistent activity undertaken in order to recover the amounts outstanding.
- In respect of performance monitoring, we confirmed that:
  - Reporting of the level and age of debt had been made to DCMS and HM Treasury between March and May 2021;
  - Management Dashboards had been produced on a weekly basis and reported to senior management.

Non-payment of DP fees

- We confirmed that the ICO has policies and procedures for its processes related to fines issued in respect of non-payment of the annual DP fee documented and available to staff on SharePoint. These are adequate in setting out processes. We did note that some did not appear to have been dated and have made a Priority 3 recommendation at Section 04.
- In June 2021, we received a list of the ten FPN's which had been issued since collection processes resumed in May 2021. We reviewed the ten FPN's and confirmed that NOI and FPN letters had

mazars

been sent within the expected timescales and fines noted within the letter were in line with the organisations recorded Tier group.

- We reviewed the ICO website and confirmed there to be a page setting out the regulatory approach during the Covid-19 pandemic.
- We reviewed weekly reports, including up to the week ending 20 August 2021, and confirmed these to have been completed and reported to senior management on a weekly basis.

3.2 Risk Management

Our review of the ICO's Risk and Opportunity Register reported to Audit and Risk Committee in April 2021 acknowledged that the ICO has established the following strategic risk of relevance to this audit:

> Risk 3 (R46) – *Financial Resilience: "Risk that sensitivities in the income growth forecast and new territories of expenditure create inaccurate financial forecasting and planning assumptions leading to insufficient funding and financial stress impeding the ICO's ability to meet its statutory requirements, and full delivery of all its intended IRSP goals and outcomes.*
> Risk rating: 12 (Amber). Target rating: 12 (Amber)

The following mitigating controls across both risks have been identified which relate to the scope of this review:

- Procedures in place to manage fee collection; and
- Weekly update on income to ET.

Based on the findings of our review, we were able to confirm that there are documented procedures in place to manage fee collection and the recovery of fines and regular reporting to senior management takes place to ensure there is oversight of income.

3.3 Value for Money

Value for Money ('VfM') is always an important factor in governmental organisations, as more scrutiny is placed on the spending of public sector organisations.

The ICO's fines recovery process demonstrates VfM through activity such as Companies House checks to ensure organisations are still trading before issuing NOIs which helps to ensure further resource and time is not used on contacting defunct organisations.

The utilisation of ICO's creditors rights and appointment of preferred insolvency practitioners aids the recovery of amounts owed by organisations put into insolvency by their Directors following the issue of fines in respect of breaches of regulated legislation that may otherwise not be recovered.

3.4 Sector Comparison

By comparing the equivalent of the fines recovery process to that of other regulators and fee/income collecting bodies we work with, we have identified common themes of good practice across the sector. These include:

- Regular engagement with organisations to recover fines at the earliest opportunity;
- The use of payment plans to assist the recovery of fines from organisations which could otherwise fall into financial hardship; and
- Working with exterior parties (e.g. the Insolvency Practitioner and Forbes) to recover unpaid fines.

In relation to our assessment of the ICO's control framework compared to those of the key themes from others within the sector, we have found that the ICO operative an effective control framework with strong processes as we have seen elsewhere.

04 Areas for Further Improvement and Action Plan

Definitions for the levels of assurance and recommendations used within our reports are included in **Appendix A1**.

We identified areas where there is scope for improvement in the control environment. The matters arising have been discussed with management, to whom we have made recommendations. The recommendations are detailed in the management action plan below.

<table>
<tr><th>Ref</th><th>Observation/Risk</th><th>Recommendation</th><th>Priority</th><th>Management response</th><th>Timescale/ responsibility</th></tr>
<tr><td>4.1</td><td>Review Dates for Policies & Procedures
Observation: We noted that most of the Policy and Procedure documents provided were dated within the past two years, with the exception of:
• The FRU Civil Case Flowchart - dated December 2018);
• Payments and Penalties Procedures (DP fees) – undated;
• Timeline and Processes for Our Work (DP Fees) – undated; and
• Payments and Penalties Bad Debt Write Off Procedures (DP Fees) – undated.
We also noted that there was not a next review date indicated on any of the documents. Noting of cyclical review dates helps to ensure that procedural guidance remains consistent with current procedures.
Risk: Incorrect processes are followed as a result of outdated procedural guidance</td><td>ICO should:
1. Review its policy and procedure documents in respect of fines issued to confirm that they are in line with current working practices;
2. Note the date of review and the individual undertaking the review within the document; and
3. Note the next expected review date within the document.</td><td>3</td><td>Accepted</td><td>September 2021. Traci Shirley and Mike Cooke.</td></tr>
</table>

A1 Audit Information

Audit Control Schedule	
Client contacts:	Steve Eckersley, Director of Investigations Mike Fitzgerald, Director of Digital, IT and Business Services Andy Curry, Head of Investigations Kerry Smith, Acting Investigations Group Manager Traci Shirley, Group Manager – Business Services - Data Protection Fees Mike Cooke, Team Manager – DP Fees (Payments and Penalties Team)
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Mark Mitchell, Senior Auditor
Finish on site/ Exit meeting:	23 August 2021
Last information received:	1 September 2021
Draft report issued:	8 September 2021
Management responses received:	9 September 2021
Final report issued:	10 September 2021

Scope and Objectives

Audit objective: To provide assurance that ICO has effective controls in place over its fines recovery processes. Our review considered the following risks:

- **Policies and Procedures** – The ICO has not set out how fines should be issued and recovered within internal policies and procedures
- **Roles and responsibilities** – The ICO has not set out roles and responsibilities for fine recovery
- **Fines issued –** Fines are not recoverable as they have not been issued correctly
- **Debt Recovery of Fines** – Fines unpaid are not chased on a regular basis.

  The ICO does not seek to engage effectively with organisations to cover fines, for example, agreement of a payment plan.

  Where fines remain unpaid the ICO does not review and/or use other collection enforcement methods.

  Where a debt payment agreement has been put in place, the ICO does not monitor payments or take action when they are broken
- **Monitoring and reporting** – The level and age of debt in relation to fines is not monitored or reported to management.

The scope for the audit is concerned with assessing whether the ICO has in place adequate and appropriate policies, procedures and controls to manage the above risks. We will review the design of controls in place and, where appropriate, undertake audit testing of these to confirm compliance with controls, with a view to forming an opinion on the design, compliance with and effectiveness of controls.

Testing will be performed on a sample basis, and as a result our work does not provide absolute assurance that material error, loss or fraud does not exist.

Definitions of Assurance Levels

Level	Description
Substantial Assurance:	The framework of governance, risk management and control is adequate and effective.
Moderate Assurance:	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited Assurance:	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory Assurance:	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
Priority	**Description**	**Action required**
Priority 1 (Fundamental)	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.	Remedial action should be prioritised and undertaken within an agreed timescale.

Statement of Responsibility

We take responsibility to the Information Commissioner's Office (ICO) for this report which is prepared based on the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Contacts

Peter Cudlip
Partner, Mazars
peter.cudlip@mazars.co.uk

Darren Jones
Manager, Mazars
darren.jones@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.co.uk