Phil Keown
Engagement Lead
T: 020 7728 2394
E: philip.r.keown@uk.gt.com

Will Simpson
Associate Director
T: 0161 953 6486
E: will.g.simpson@uk.gt.com

Robert Jebbett
Executive
T: 0161 953 6346
E: robert.jebbett@uk.gt.com

Information Commissioner's Office

Internal Audit 2016-17: Recovery of Monetary Penalties

Last updated 20 October 2016

Distribution		**Timetable**	
For action	Enforcement Group Manager	Fieldwork completed	19 September 2016
		Draft report issued	23 September 2016
For information	Senior Corporate Governance Manager	Management comments	20 October 2016
	Audit Committee	Final report issued	20 October 2016

Contents

Glossary

The following terms are used in this report:

DCMS – Department for Culture, Media and Sport

1 Executive Summary

1.1 Background

As part of the 2016-17 Internal Audit Plan, it was agreed with the Audit Committee and management that we would deliver a review of the ICO's approach for the recovery and collection of unpaid Civil Monetary Penalties (CMPs).

The ICO has the power to levy fines against organisations for serious breaches of the Data Protection Act (DPA) or the Privacy and Electronic Communications Regulations (PECR). A clear process exists for the levying of such penalties.

During 2015-16, the ICO issued a total of 22 final notices, with a total value of £2.5 million. Already this year, through Quarter 2 2016-17, 16 final notices with a total value of £2.02 million have been levied. In the past, the majority of penalties were levied against public bodies for breaches of DPA and therefore payment was rarely considered to be a problem. However, a greater number of penalties are being issued against commercial organisations, some of whom are run by unscrupulous individuals who fail to pay the penalties levied.

While the ICO is responsible for collecting the Monetary Penalties that it levies, all monies received are paid into HM Government's Consolidated Fund.

1.2 Scope

Our review involved an assessment of the following risks:

- The ICO may not operate a clear and robust process for monitoring the collection of Monetary Penalties resulting in the failure to identify old debts and take appropriate action to collect outstanding monies;
- The ICO may not operate a structured process for taking follow up action against non-payment of Monetary Penalties (including the engaging of third parties in debt collection activities) resulting in a failure to collect unpaid monies in a timely manner, and the inconsistent treatment of outstanding debts and the inconsistent use of external legal counsel, bailiffs and the Insolvency Service;
- The ICO may not monitor and report on its performance in collecting Monetary Penalties resulting in a failure to understand the success of individual follow up activities and to identify opportunities for enhancing its education of external organisations and an inability to demonstrate its effectiveness in collecting debts on behalf of DCMS and HM Government.

Further details on responsibilities, approach and scope are included in Appendix A.

1.3 Overall assessment

We have made an overall assessment of our findings as:

Overall assessment	
We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.	Green

Please refer to Appendix B for further information regarding our overall assessment and audit finding ratings.

1.4 Key findings

Risk / Process	High	Medium	Low	Imp
Monitoring Collection of Penalties	-	1	-	-
Follow-Up of Non-Payment	-	-	3	1
Monitoring and Reporting of Performance	-	1	-	-
Total	**-**	**2**	**3**	**1**

The following findings are assessed as Medium:

- The ICO does not have any overall guidance in place for the end to end processing and management of CMPs. Such guidance should set out instructions for the registration, monitoring and management of penalties levied and the treatment and escalation of non-payment which may eventually lead to formal legal action. We would expect formal policies and procedural documentation be developed that sets out the full requirements for the issuing of CMPs and the subsequent collections of monies, clearly defining roles and responsibilities where decisions are required and referencing supporting databases or spreadsheets.
- The Enforcement team does not formally report on CMP operations, such as casework under way, final notices issued, ongoing legal action and collections activity. Further, although we acknowledge that the benefits to pursuing penalties through legal process are not solely financial, there is also no cost/benefit reporting of legal costs incurred compared to the amounts of recoveries made through court action. With the increased focus on compliance with both data management and electronic communications regulation, and the introduction of the General Data Protection Regulation (GDPR) in 2018 resulting in a larger future caseload, we would expect that operational CMP reporting would clearly support Senior Leadership Team and management decision making (e.g. resourcing levels, setting of early payment discount percentages or pursuing CMPs through the insolvency process.)

1.5 Basis of preparation

We identified the following controls in place during our audit:

- The ICO maintains a bank account income suspense account which is reconciled on a monthly basis. Any items that appear in this account are reviewed and posted to the correct account by the Accounts Administrator;
- The ICO has an up to date Bad Debt policy that was finalised and agreed by the Information Commissioner in November 2015 and issued via the Finance Steering Committee;
- Where debt recovery action is to take place following a non-payment of a CMP, legal advice (both from qualified internal teams and from external experts) is sought;
- On a monthly basis, the Head of Finance completes a management report that summarises the current position of the CMP debtors accounts for the Finance Steering Committee and Senior Leadership Team.

1.6 Elsewhere in the sector

We detail below other ways of working and commonly occurring issues that we have experienced during similar types of reviews for other bodies. The following does not necessarily purport to be good practice but is included for your information and consideration:

- Other similar bodies will also develop a set of KPIs or targets to measure the success of the accounts payable and debt recovery process. Where targets are under threat of achievement (such as high cost of recovery), management recovery plans will be developed and implemented.

1.7 Acknowledgement

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit.

2 Detailed Findings

2.1 The ICO may not operate a clear and robust process for monitoring the collection of Monetary Penalties

1.	Medium	Guidance and procedural documentation

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
The responsibility for the management and monitoring of CMPs is currently in transition to the Enforcement Group. As part of this transition, two main policy documents have been developed: the 'Bad Debt' policy, and 'Guidelines on Instructing Insolvency Practitioners in respect of Unpaid Monetary Penalty Notices'. There is however, no overall guidance and procedural documentation for the end to end processing and management of CMPs that sets out: • Instructions for the setup, monitoring and management of penalties levied; • Communication with organisations and individuals; • Managing payments received; • Setup and monitoring of payment plans; and • The treatment and escalation of non-payment (eventually leading to management decision making on legal advice and perusal of court action). As a consequence, whilst those that are involved with the issuing of CMPs know their roles and responsibilities, there is a risk that individual cases may not be progressed in the most efficient or effective manner, and that the management of debt may be taken forward without appropriate authority.	ICO management should develop formal policies and procedural documentation that sets out the full end to end process that is required to be carried out for the issuing of CMPs and the collection of monies (including roles and responsibilities where decisions are required and reference to supporting databases or spreadsheets).	*Agreed action* *Date Effective: 30.11.16* *Owner: Andy Curry* *Draft guidelines have been drafted to support the current recovery pilot project, and an overarching policy with supporting process documentation will also be drafted taking into account any lessons from the pilot work.*

2.2 The ICO may not operate a structured process for taking follow up action against non-payment of Monetary Penalties

2.	Low	Monitoring and management of CMPs

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
To track and monitor 'live' CMPs, both the Enforcement and Finance team maintain separate spreadsheets that together contain all relevant operational and financial details. The Enforcement team use this information to review CMP due dates, with those remaining unpaid (despite appeals and expiry of the due date) being escalated to the Head of Enforcement for a decision on further action. Our review of a sample of CMPs issued during 2016 found that all had been monitored and followed up where required, but identified the following issues: • A review of cases on the CMP register takes place manually, rather than being driven by automatic diarised reminders; • Following the expiry of a CMP's 'due date', the ICO does not have a process in place to issue reminder letters to the organisation or individual. Instead, if the Enforcement team confirm that no payment has been made and no correspondence has been received, the case will be immediately escalated to the Head of Enforcement to authorise an application for a court order; • In reviewing those cases where a payment had been made to clear the CMP, we identified that the ICO does not issue a final remittance advice or CMP closure notice to the organisation. There is a risk that, in relying on a manual monitoring, not issuing 'final payment notices' or reminders nor confirming case closure with organisations, the ICO may not be administering the CMP process in the most effective manner, ultimately resulting in cases not being followed up on a timely basis or incurring unnecessary legal and administration costs.	ICO management should develop CMP management processes to implement: • A CMP due date monitoring process that is shared across the Enforcement team (for example a shared Microsoft calendar) and which is not dependent on an individual's availability or workload. • A single CMP management spreadsheet / database that contains all relevant information for managing CMPs effectively (including case references and details, debtor amounts, expected credits, payments confirmed as received, cases moved to debt collection or overdue debtors). • A set of 'overdue debt' letter templates for both Data Protection and PECR fines. These templates should include details such as methods of payment and timescales in which the overdue payment should be made and clearly set out the enforcement actions that the ICO will pursue together with individual and organisational impacts. • A standard 'CMP closure' letter to confirm receipt of payment and the closure of the ICO case. In the case of CMPs where payment plans have been in place, this should list all the payments made and confirm complete closure.	*Agreed action* *Date Effective: 30.11.16* *Owner: Andy Curry* *This work will form part of the end-to-end process documentation to be developed as set out in 1 above.*

3.	Low	Accounting for Civil Monetary Penalties

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
CMPs are required to be posted by the Finance team to the ICO's ledger at the full and final value of the penalty. Early payment discounts of 20% are applied as a credit where payment is made within 28 calendar days of the date of the final notice. If an organisation appeals against the penalty, they are not entitled to the discount. We reviewed a sample of 10 CMPs (5 DPA penalties and 5 PECR penalties) issued in the last year. In 9 of the 10 cases, the CMP raised matched that in the ledger. However, in the one exception, the debt had been posted to the ledger incorrectly at the discounted value of £144k (which was the amount paid), not the full value of the penalty of £180k. In not posting the correct CMP value of to the ledger (and subsequently not posting a credit note to register the early payment discount), both the value of the CMP debtors that are reported and the early payment discounts that have been claimed are incorrectly recorded.	Finance staff should be reminded that, when posting CMP amounts to the debtor ledger, the full agreed notice amount should be recorded, with any early payment discount or adjustments being applied as separate transactions.	*Agreed action* *Date Effective: 12.10.16* *Owner: Andy Curry/Sally Hanson* *Finance have been provided with access to the Enforcement master spreadsheet, and will add reporting information to that spreadsheet.*

4.	Low	Treatment and monitoring of 'payment plans'

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Whilst the ICO does not proactively offer payment plans or split payments to encourage prompt and full payment of CMPs, the Enforcement team will communicate with data controllers about payment options following delivery of a final notice. The Head of Enforcement will ultimately authorise any decision to split a CMP into multiple payments, taking into account a number of factors such as cash flow, reputational standing of the organisation, past history of compliance, etc. There is however, no formal template for the Enforcement team to use to register and manage a 'reducing balance' CMP. In addition, there is no formal monitoring for part payments; instead the Enforcement team rely on the team leaders to manually update the CMP balance and due date for the next instalment on the register of monetary penalties when a payment is received. In not maintaining a standard template agreement, or a formal agreed process, there is a risk that part-payments towards a CMP may not be accurately recorded and that agreements may not be effectively monitoring resulting in late payments not being highlighted and escalated for focused debt collection activity.	As part of the development of the formal CMP policy and procedures documentation, the Enforcement team should develop the process by which payment agreements are set up and managed, together with the implementation of a standard template for payment agreements which includes the original balance and lists the agreed payment dates and payment amounts.	*Agreed action* *Date Effective: 30.11.16* *Owner: Andy Curry* *This work will form part of the end-to-end process documentation (see 1 above).*

5.	Improvement	Authorisation for legal advice and court orders

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
When it is confirmed that a company in receipt of a CMP has not paid by the due date and no appeal has been lodged, the case is reviewed by the Head of Enforcement and formal authorisation is provided to begin recovery action. We confirmed that evidence of this review is retained in each case file. Our review of the two current recovery cases on file found that this authorisation is obtained via an email chain, rather than a formal decision template. Whilst in both cases, the email contained a clear rationale for the decision to process with legal action, the process would be more effective if all escalation decisions were recorded on a formal template that documents: • CMP details; • Rationale to pursue legal action (e.g. repeat offender, company set up solely to operate illegally, etc.); • Approximate costs of taking case forward (both to court order and potentially specialist recovery agents). There is a risk that, in not formally documenting the decision to escalate a case to formal court action or litigation, not all pre-recovery actions may have taken place, or the required management authority may not have been provided to incur legal costs.	The ICO should develop a formal 'escalation to legal action' template for completion by the enforcement team and sign off by the appropriate manager. These documents should be completed for each case taken where a debt is not to be immediately written off, but to be taken forward for legal advice and debt recovery	*Agreed action* *Date Effective: 17.10.16* *Owner: Andy Curry* *A formal decision record has been incorporated into the new Enforcement Report template, which will be introduced from 17.10.16.*

2.3 The ICO may not monitor and report on its performance in collecting Monetary Penalties

6.	Medium	Development of Operational Reporting

Finding and Implication	Proposed action	Agreed action *(Date / Ownership)*
Finance collate information on the current financial position of Monetary Penalties owed to the ICO, total penalties issued during the year, prompt payment discounts applied, payment receipts any bad debt provisions or impairments to be made which is reported monthly through the Finance Steering Group. There is, however, no formal reporting on Enforcement operations, casework, legal action under way and collections. Further, although we acknowledge that the benefits to pursuing penalties through legal process are not solely financial, there is also no cost/benefit reporting of legal costs incurred compared to the amounts of recoveries made through court action. With the increased focus on compliance with both data management and electronic communications regulation, and the introduction of the General Data Protection Regulation (GDPR) in 2018, without effective operational reporting on the management of the CMP process, there is a risk that decisions may be made that result in an unnecessary expense being incurred, for example, incorrect resourcing levels, setting excessive early payment discount percentages, or incurring excessive legal fees through pursuing unenforceable penalties through the insolvency process.	Using information that is already available or collated by the Enforcement and Finance teams, a Monetary Penalty dashboard should be developed for reporting to the Leadership Committee and Management Board. This dashboard should contain additional information on: • Current position of casework; • Ongoing investigations; • Points of interest to note (for example increases in certain case types); • Trend analysis of penalties levied and collected by case type (e.g. data protection or PECR - Privacy and Electronic Communications Regulations); • Volumes and values of 'early payment discounts' applied to CMPs; • Collection success rates; • Number of legal cases currently in train; • Number of penalties written off as unenforceable; • Costs incurred vs recoveries by recovery partner.	*Agreed action* *Date Effective: 31.12.16* *Owner: Andy Curry* *The action is agreed, and a template will be developed for reporting to the Finance Steering Group. The aim is to introduce a formal reporting process for the start of quarter 4.*

A Internal audit approach

Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

Our audit was carried out in accordance with the guidance contained within the Government's Internal Audit Standards (2013) and the Auditing Practices Board's 'Guidance for Internal Auditors'. We also had regard to the Institute of Internal Auditors' guidance on risk based internal auditing (2005). In addition, we comply in all material respects with other Government guidance applicable to Public Bodies and have had regard to the HM Treasury guidelines on effective risk management (the 'Orange Book').

As part of the 2016-17 Internal Audit Plan, we agreed with the Audit Committee and management to deliver a review of the ICO's approach for the recovery / collection of unpaid Monetary Penalties from organisations.

Our aim in completing this audit was to ensure that the ICO has appropriate arrangements in place to identify, manage and report on risk.

We achieved our audit objectives by:

- Meeting with the individuals responsible for setting, monitoring and implementing the Monetary Penalties collection process to identify the control structure in place;
- Seeking evidence to confirm the operation of understood controls, including sample testing where appropriate;
- Testing a sample of Monetary Penalties levied to evaluate whether the appropriate process had been followed.

The findings and conclusions from this review will support our annual opinion to the Audit Committee on the adequacy and effectiveness of internal control arrangements.

Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations, therefore references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should therefore maintain

sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

Scope

Our review involved an assessment of the following risks:

- The ICO may not operate a clear and robust process for monitoring the collection of Monetary Penalties;
- The ICO may not operate a structured process for taking follow up action against non-payment of Monetary Penalties (including the engaging of third parties in debt collection activities);
- The ICO may not monitor and report on its performance in collecting Monetary Penalties.

Additional information

Client staff

The following staff were consulted as part of this review:

- Andy Curry – Enforcement Group Manager;
- Mark Thorogood – Solicitor Group Manager;
- Sally Hanson – Interim Head of Finance;
- Dave Clancey – Enforcement Team Leader.

Documents received

The following documents were received during the course of this audit:

- Bad Debt Policy (November 2015);
- Draft guidelines for unpaid Monetary Policy Notices and instructing insolvency practitioners;
- Enforcement monetary penalty masterfile (redacted);
- Finance civil monetary penalty reconciliation (March to July 2016);
- Payment receipts Suspense Account report (September 2016);
- Finance Steering Group papers (October 2015, November 2015, March 2016, May 2016, July 2016).

Locations

We visited The Information Commissioner's Office, Wilmslow for this review.

B Overall assessment and audit issues rating

Overall assessment

Rating	Description
Red	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which should be raised with Senior Management and the Audit Committee at the earliest opportunity.
Amber	Following agreement of the nature and significance of individual issues with management, in our view this report contains matters which require the attention of management to resolve and report on progress in line with current follow up processes.
Green	We have identified matters which, if resolved, will help management fulfil their responsibility to maintain a robust system of internal control.

Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

Rating	Description	Features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management	• Key control not designed or operating effectively • Potential for fraud identified • Non compliance with key procedures / standards • Non compliance with regulation
Medium	Important findings that are to be resolved by line management.	• Impact is contained within the department and compensating controls would detect errors • Possibility for fraud exists • Control failures identified but not in key controls • Non compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures.	• Minor control weakness • Minor non compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or best practice advice	• Information for department management • Control operating but not necessarily in accordance with best practice

Grant Thornton

An instinct for growth™

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grant-thornton.co.uk