Annual Breach Management Cases Report – 2022/2023

Introduction

The responsibility for managing breaches of the Landfill Tax Regulations 1996 (Regulations) is split between Entrust and our Commissioners, HM Revenue & Customs (HMRC). Entrust is appointed by HMRC as the Regulator of the Landfill Communities Fund (LCF) and as part of that role as set out in our Terms of Approval (TOA) with HMRC, Entrust manage any breaches of the Regulations, Conditions or our guidance, attempting to resolve them before, ultimately, in very serious cases EBs' are referred to HMRC for clawback or enforced revocation.

This document lists breaches that have arisen and have been managed during 2022/2023, with detail on how these types of cases can be, or have been resolved.

In 2022/2023, seven new cases had arisen that required full breach management case files to be opened for investigation. compared with two in 2021/2022. This is mirrored by the rise in cases dealt with through compliance reviews without the need for referral to breach management as seen in the quarterly report, and other cases found from other areas of operation, which were resolved with the EB's before the case turning into a full breach case.

Entrust believe there are two possible reasons for the 2022/2023 increase in breach management cases. Firstly, the Pandemic and Cost of Living Crisis, both of which had or continue to have a significant impact on EB project delivery. Secondly, with the introduction of Project Site Visits in November 2021 which provides increased scrutiny of completed projects, more breaches have been discovered, leading to conversations with EBs regarding project monitoring and due-diligence. Entrust continue to work with EBs to establish best practice, to improve the general compliance of project monitoring and spending. This advisory document seeks to achieve this by listing the cases, anonymously, to inform and help EBs to develop quality processes that mitigates the risks of breaching the Regulations and Entrust guidance.

There are eight cases by types listed below which detail the breaches we have managed in the past year, which were not resolved through the normal compliance review process. This means that there may have been other breaches or guidance findings of the same type, but they have been resolved without referral to the breach management team and so are not included in this report. Details of findings of the compliance reviews can be found in the quarterly report found alongside this report on the website. Each case is assessed, or is being assessed, on their own circumstances, and if any resolutions have been listed, this will have been due to various factors or mitigations.

The information listed below give a brief description of how Entrust has approached different types of breaches. More information on our breach framework can be found on our website. If you would like more suggestions as to how to mitigate any risks of non-compliance as a result of this information, please contact us.

Appendix A below sets out the type of breach, number of instances and the Regulations or guidance that has been breached.

1. Case Type #01 – Not responding to Information Requests

1.1. One of the more common forms of breach is when an Environmental Body (EB) does not respond to a request for information.

1.2. There were three cases in 2022/2023, each resolved by informing the EB, when contact was established, that they need to improve their processes to respond to any information request in a timely manner, and within the timeframe stipulated by the request.

1.3. These cases can vary in monetary value, ranging from information regarding a late form, to significant value of invoices missing from project reviews.

1.4. Most cases are concluded before a formal breach case is opened by applying several methods by Entrust, as set out in our internal policies, which are followed before any action is taken. In the most serious cases, where after several attempts across a number of months, the EB has not responded, or cannot be contacted, a breach case would be opened, going through the four stages as set out in the breach framework in sequence

2. Case Type #02 – Projects that had to close after completion

2.1. This form of breach occurs when an EB completes a project under Object D or E, often without any breaches up to the point of completion, then at some point within the monitoring period, the project cannot, for whatever reason, continue to operate as a public amenity. There have been three instances where this has arisen as being one of the factors in 2022/2023, and we feel that there may be more cases of a similar nature arising during the following year.

2.2. The resolution to this type of case is challenging, due to mitigating circumstances being instrumental to the proportionate and appropriate actions. Action on cases such as these include attempts to bring the project back into a compliant state, or if this is not possible, recover the value of the project or assets depending on what is viable.

2.3. Such cases can also arise due to a lack of due-diligence or lack of business case resulting in offers of funding to unstable, or insecure organisations. It is suggested that good practice would include a framework that ensures recipients of LCF funds are financially secure (going concern) and well managed.

3. Case Type #03 – Invoices insufficient, a connected party or potentially fraudulent

3.1. There are two cases that arose during 2022/2023 that were deemed serious enough for breach management cases. These cases involved an EB paying funds on invoices that did not provide sufficient quality of evidence, and on investigation, were found to be potentially fraudulent or awarded to a connected party such as an applicant's director.

3.2. In this matter, the resolutions may differ depending on the factors involved, and whether the funds are easily recovered. It is suggested that EBs have a robust checking process, which includes verification of the supplier/contractor, before funds are paid out to an applicant.

4. Case Type #04 – Project aims/objectives, and public access statement errors/inaccuracies

4.1. This case type has been part of one longer running case and three new cases that arose in 2022/2023. When visiting a project, the compliance team have discovered that the project that was delivered did not match the project aim, and is not available to the public for the times registered on project applications. Information provided (at registration was either an error, or in more serious cases, deliberately written with false or exaggerated information to make the project less likely to be queried.

4.2. Applications have also overstated the public nature of the facility, and in reality, are intended to be used by a specific user, or for restricted uses.

4.3. Entrust would emphasise that the accuracy of information on project application and completion forms is maintained at a high standard, and accurately represents the project to be delivered. We would also request, where it is not clear, the applicant provides some form of evidence of community participation and a business case, especially when the facility is on a restricted premises such as a school, to show the public will have the necessary access to the facility, for the facility to qualify as a public amenity as required by the Regulations.

5. Case Type #05 – Changing the aim and items of projects without notifying Entrust

5.1. There have been a number of cases of this nature dealt with through compliance reviews, but two have been serious enough to refer them as a breach management case. The Regulations and Conditions outline how funds must only be spent on items approved by Entrust. Therefore, items added to the project without Entrust prior approval are non-compliant.

5.2. In the majority of cases, adjusting an aim, or adding items are approved, providing they are clearly related to the project that was registered. All that is required is confirmation in writing, prior to any spending on these items.

5.3. These cases can be difficult to resolve due to the nature of funds having been already spent. Therefore, we would stress the importance of checking the project registration matches any claim for funding and invoices provided, before agreeing to transfer any funds to an applicant.

6. Case Type #06 – Administration fees for management of projects paid to another EB

6.1. In 2015, the regulations were amended, removing Object F, which allowed one EB to provide services to administer the funds of another EB. There were two cases in 2022/2023 where this breach was identified.

6.2. These cases can be complex, and involve a number of factors, meaning that resolutions to the breach can differ. We would stress that any transfer of funds between EBs that is not for the purpose of project spending is unlikely to be a compliant transfer without prior approval of special cases, such as when one EB is revoking and has unspent funds.

7. Case Type #07 - Late forms for contributions and fund transfers

7.1. The regulations specify that any transfer of funds between EBs, or any contribution received must be reported to Entrust within seven days of the date of transaction. Most breaches of this nature require an advice and guidance letter, or warning letter if a second occurrence of a breach in any 12-month period.

7.2. There are on occasion, but not in 2022/2023, instances of repeated behaviour that have required further action, such as a meeting with the chair of the EB and main contact. Due to there being no monetary value involved, this breach does not involve any potential for clawback of funds.

7.3. There were 31 cases of this type in 2022/2023.

8. Case Type #08 - Spending outside the Prescribed Period (SOPP)

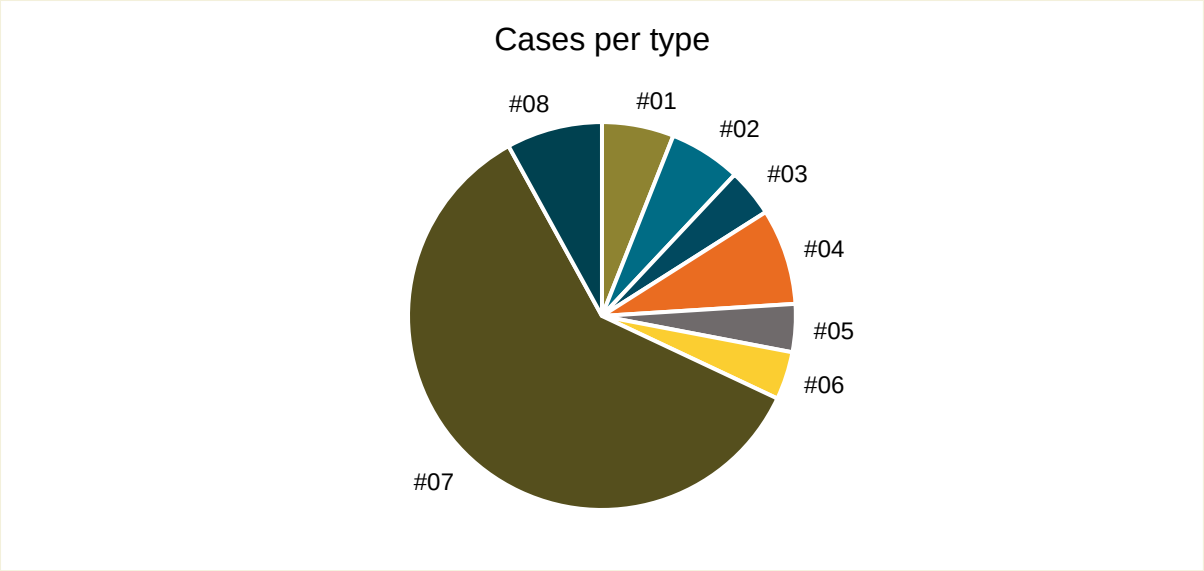
8.1. This breach arises when the EB spends funds outside of the project dates set by the project approval.

8.2. These breaches can vary in seriousness, both in material value and in scope. Small breaches of a few days are usually dealt with through guidance, but on occasion, the repayment of funds may be deemed appropriate due to the seriousness and materiality.

8.3. There were six SOPP breaches in 2022/2023, with one EB case escalated as a more serious case due to multiple simultaneous breaches.

9. Further details

9.1. From the number of cases for each case type, as shown in the chart below, the most common breach is filing late forms, as may be expected. However, there have been several Case #04 and Case #08 breaches. These are more serious, often have monetary value and contravene the Regulations. They are also both most commonly errors in administration or awareness of the requirements.



9.2. We would, therefore, like to draw your attention particularly to case types #08 and #04, to look at your EB processes and procedures to ensure the risk of breaching the regulations in this way is low.

9.3. However, with over 1,700 enrolled EBs, and over 1,000 projects per year, the total count of 49 cases requiring breach management action is an indication that overall, the majority of operation in the scheme is done within compliance of the Regulations, Conditions and Entrust guidance.

9.4. If you would like any further information on the way Entrust manage breaches, please contact us at helpline@Entrust.org.uk

Entrust

April 2023

Appendix A – Breaches of the Regulations and/or Entrust Guidance

Case	Breach	Number of instances	Regulation/Guidance breach references
#1	Not responding to Information Requests	3	34.-(1)(i) 33A.-(1)(d-i) Guidance Manual 3.8 - 3.11
#2	Projects that had to close after completion	3	33.-(2)(d) 33A.-(1) Guidance Manual 5.8
#3	Invoices insufficient, a connected party or potentially fraudulent	2	34.0(1)(i) Guidance Manual 5.3 and 3.1.1
#4	Project aims/objectives, and public access statement errors/inaccuracies	4	33.-(2)(a-e) Condition 1)(2)(b) Guidance Manual 4.3.3
#5	Changing the aim and items of projects without notifying Entrust	2	33.-(2)(a-e) Condition 1)(2)(b) Guidance Manual 4.6
#6	Administration fees for management of projects paid to another EB	2	33.-(2)(f) (removed in 2015) Guidance Manual 3.12
#7	Late forms for contributions and fund transfers	31	33A.-(1)(e) Guidance Manual 3.8
#8	Spending outside the Prescribed Period	6	Condition 1) (1)(c) and (2)(a) Guidance Manual 5.4