ofgem e-serve

Policy/Guidance

Fraud Prevention Strategy for the GB and NI Non Domestic Renewable Heat Incentive Scheme

This paper sets out the means by which Ofgem will fulfil its responsibility to manage fraud, non-compliance and abuse within the GB and NI Non Domestic Renewable Heat Incentive Scheme.

Author Ade Obaye

December 2013

Contents

1. Introduction

1.1 This document describes the key elements of the Non Domestic Renewable Heat Incentive (NDRHI) Fraud Prevention Strategy. It has been reviewed by Deloitte as part of the review of NDRHI Systems and Processes, which took place in July/August 2011. The document was updated in August 2012 to include the Northern Ireland NDRHI scheme.

2. Background

2.1 The NDRHI is an environmental programme introduced by the Government designed to promote the widespread uptake of renewable heat generation technologies at the commercial and industrial scales. It is the first scheme of its kind worldwide, intended to encourage a radical change in the way we generate heat by bridging the gap between the cost of conventional and renewable heat systems at all scales, taking UK demand of renewable heat from 1% of total heat demand to 12%. A Domestic RHI scheme will be launched in 2014.

2.2 DECC estimates the RHI will deliver an additional12,000 heat generation installations by 2015 and DETI estimates the NI RHI will deliver an additional 360 heat generation installations by 2015. Dealing directly with and making payments to such large numbers of consumers is new to Ofgem and does not fall within its normal core area of business.

3. Scope and limitations

3.1 This Fraud Prevention Strategy is a high-level overview of the RHI fraud threats and seeks to provide assurance on the adequacy of the measures in place to prevent the opportunity for fraud and non-compliance, detect fraudulent or non-compliant activity and enforce sanctions when appropriate.

3.2 This Fraud Prevention Strategy has a wider scope than activities that fall within the strict definition of fraud. Gaming opportunities and abuse of the system is also considered however, it should be noted that under the RHI Regulations for both the GB and NI schemes, our power to investigate, request information and take enforcement action is limited to participants and does not extend to third parties such as installers and manufacturers.

4. Definition of Fraud

4.1 For the purpose of this document, the act of fraud is as stated in Ofgem E-Serve's Fraud Policy (Ref. FRM04/2012):

'...activity aimed at securing a gain, causing a loss, or exposing somebody to the risk of a loss, through false representation, failing to disclose information, or through abuse of position...'

4.2 For a person to have committed fraud, they must have acted dishonestly and with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of a loss) on another.

4.3 For the RHI, examples of fraud would include falsifying meter readings/periodic data submissions, submitting false documentation is support of an RHI application, submitting applications for bogus, non-existent installations or an Ofgem member of staff diverting RHI support payments to their own bank account.

5. Fraud Response (including Enforcement)

5.1 The action taken when we uncover suspected fraud or non-compliance within the RHI will depend on the seriousness of the fraud or non-compliance.

5.2 We have recourse to a range of sanctions that we can enforce including temporary suspension of payments under the scheme, reducing or withholding payments and exclusion from the scheme. Any sanction applied would be in accordance with the RHI Regulations[1].

5.3 Where, due to the nature of the non-compliance uncovered, we are unable to rely on data being provided and are therefore unable to calculate payments, we are not able to impose a sanction on future payments. In such cases, we will advise the participant that we are unable to make payments and require them to rectify the situation to our satisfaction before payments can continue.

5.4 Due to limitations in our statutory powers, we are not able to conduct criminal investigations. It is expected that majority of breaches that will occur in the RHI will be dealt with via the compliance route while the more serious and deliberate attempts to cheat the system will be referred to the appropriate authorities via the Action Fraud online reporting tool for their consideration of conducting a criminal investigation. This will not prohibit Ofgem from also enforcing any of the sanctions detailed in the RHI sanction policy (Appendix 2).

5.5 Fraudulent cases involving Ofgem staff will be dealt with in accordance with Ofgem E-Serve's Fraud Policy (Ref. FRM04/2012).

6. Stakeholders/agencies

6.1 The main stakeholders/agencies associated with RHI fraud prevention and the outcomes of the association are:

[1] Renewable Heat Incentive Regulations 2011and Renewable Heat Incentive (Northern Ireland) Regulations 2012

6.2 National Fraud Authority (NFA)[2]:

- Had an input in developing the RHI fraud risk register and provided advice on government best practice on fraud prevention/detection, including providing useful contacts within the Serious Organised Crime Office (SOCA)[3] and the Department of Works and Pensions;

- Created and implemented a new Home Office Counting Rule that will enable Ofgem (and other Government departments) to report suspected fraud via the Action Fraud online reporting tool;

- Delivered training to Ofgem Fraud Prevention Managers on how to use the Action Fraud tool; provided initial support in the development of an E-learning Fraud Awareness toolkit for E-Serve staff and delivered workshops during Fraud Awareness week.

6.3 Serious Organised Crime Agency (SOCA):

- We worked jointly with SOCA to put measures in place to prevent access by organised criminals and money launderers;

- We held workshops with SOCA and outcomes include changes made to the RHI IT system to strengthen our fraud controls, provision of both Amberhill (details of known fraudulent identities) and Fraudulently Obtained Genuine (FOG) data so that we can periodically check both against our RHI applicant details.

6.4 Department for Work and Pensions (DWP):

- We consulted with the DWP regarding risks associated with making payments directly to a large number of participants. In particular, the DWP gave valuable advice on how to approach the issue of identity verification and bank account validation.

6.5 Fraud Prevention and Audit Managers Group:

- This group meets bi-monthly and its purpose is to promote best practice, share experience, help maintain relationships with other fraud prevention managers and act as a forum for discussion of common issues and barriers.

6.6 Fraud Prevention, Audit & Governance Team:

- Share best practice for the identification, prevention and escalation of fraud within Ofgem Environmental Programmes.

- Peer review of Fraud Prevention strategies and Fraud Risk Registers

6.7 Department of Energy and Climate Change (DECC):

- Set Ofgem legislative powers for investigation and imposition of sanctions;

- We are involved in the new DECC/OFGEM Fraud and Risk Working Group which has been set up to develop a suitable framework and procedure for the rapid and effective exchange of information on suspected scheme abuse, misuse or fraud, including fraud risk identification and management. We are piloting a counter fraud

[2] The National Fraud Authority will be disbanded from March 2014 and its functions will be split between the National Crime Agency, City of London Police, Home Office and the Cabinet Office.
[3] The Serious Organised Crime Agency is now part of the newly formed National Crime Agency

agreement on the NDRHI scheme, which will be rolled out to cover all schemes in due course.

7. Threats and Prevention Measures

7.1 In accordance with best practice, Ofgem supports and maintains an anti-fraud framework across the organisation. This includes having established general anti-fraud controls, a competent internal audit programme, mandatory fraud awareness training for E-Serve staff, a fraud policy, a whistleblowing policy and an employee Code of Conduct. With this framework in place, an anti-fraud culture already exists within Ofgem.

7.2 Due to the size of the RHI scheme and the large amount of public funds involved, there is a significant risk of fraud and non-compliance both from within and outside Ofgem. Possible sources are shown in Table 1 below.

Table 1: possible sources of fraud

Internal	Participants	Contractors	Criminals
Ofgem staff	Participants	Site Auditors	Organised criminals
	Independent Report on Metering Arrangements (IRMA) authors	Consultants	Opportunistic criminals
	Installers	Identity and bank validation service provider	Computer hackers
	Manufacturers		

7.3 The RHI Fraud Risk Register (RHI Fraud Risk Register) identifies a number of areas where the risk of fraud within the RHI might arise. A selection of the higher rated amongst these risks with a summary of the controls in place are:

RHI specific threats

- **Risk that the scheme may be targeted by organised criminals/money launderers**.

  Prevention: We have worked with the Serious Organised Crime Agency to put in place measures to mitigate this risk. This included holding joint workshops to get a better understanding of how organised criminals might infiltrate the RHI; establishing a process for Ofgem to be able to check new RHI participants details against lists of known fraudulent identities (Amberhill database); and also against their of Fraudulently Obtained Genuine (FOG) identities database to identify high-risk participants for more in-depth review or audit as required. We also use a third party provider to verify Authorised Signatory identities to ensure that they are genuine.

- **The risk of participants providing false metering or periodic data information in order to increase the level of RHI support payments they receive**

Prevention: The requirement that 'multiple' installations larger than 45kW capacity and all installations over 1MWprovide an Independent Report on Metering Arrangements (IRMA) as part of the accreditation process will help to mitigate the risk of accrediting both a) incorrectly designed systems and b) systems where the meters have been inappropriately calibrated; There are pre-programmed values in the RHI database for how much heat an installation could plausibly generate - if any periodic data falls outside this range an exception will appear. All exceptions are checked by the Periodic Data Submissions Team; The RHI website has a link to B&ES to metering code of practice; Information on correct meter configuration is included in our Guidance document; There have been Regulatory changes to streamline metering requirements; Photographic evidence of opening meter readings is requested as part of desk top audits; Uploading of corroborating photographs of meter readings will be required once a year as part of system improvements to be introduced in March 2014.

The risk that participants may purposefully generate unwanted heat purely to claim RHI support payments, which is in breach of the RHI regulations.

Prevention: Measure in place to mitigate against this risk include the functionality of the RHI IT system to auto-identify when the declared capacity of a new installation is inconsistent with the capacity of the equipment it has replaced, checking (during inspection audits), where installations have a heat rejection facility, that it is properly metered. Also, through discussions with DECC, the wording of the Regulations has been amended to clarify what is classed as eligible heat and clearly states that participants must not "generate heat for the predominant purpose of increasing their periodic support payment". In addition, the tiered tariff for biomass (a higher tariff rate is paid for the first 15% of annual heat generation hours) reduces the incentive to purposefully generate then waste heat.

Internal threats

- **The risk that an Ofgem staff member fraudulently manipulates the RHI IT system to divert payments into other bank accounts or otherwise misuses confidential personal data held on the system.**

  Prevention: There are suitable controls on the RHI IT system and segregation of duties to prevent unauthorised use of the system; A third party provider is used to carry out Authorised Signatory identity and bank account verification for all new applications (and when we are notified of a request to change any of these details). In addition, participant bank details are stored in a separate database and system with only key identified staff allowed access; Bank details are sent in by post and stored securely - in both a locked mailbox and filing cabinet with access restricted to key staff; Payments are only made into accounts that are in the owner's name. All requests for a change in bank details are processes by the Fraud and Compliance team who contact the Authorised Signatory to verify confidential information before making the change.

  Further preventative controls include: Increased focus on fraud and compliance in Ofgem with the creation of the Fraud Management Group and Fraud & Audit Managers Forum; Mandatory fraud awareness staff training and development of fraud prevention micro website by the Fraud Prevention, Audit and Governance Team; 10% Delegated Authority sample checks of all Periodic Data Submissions; 10% Delegated Authority sample checks of all

approved payments; All estimated data cases are agreed at band C level and all Periodic Data Submission account managers are permanent staff;

- **The risk of bribery or corruption of Ofgem staff, which may lead them to collude with a participant using their knowledge to set up new accounts or circumventing inbuilt controls.**

  Prevention: Fraud awareness training for staff, controls such as segregation of duties and suspicious item matching are built into the RHI IT system. In addition, the Fraud & compliance Team sample check a percentage of all accreditations. We are currently developing an automated management information tool, which will help to identify any anomalies in the system. Recently launched whistleblowing policy and mandatory whistleblowing training for all staff. There is also a segregation of location – periodic data assessments are carried out in Glasgow and the payments team are located in London.

Gaming opportunities

- **Participants may generate heat for eligible purposes but which do not meet the spirit of the RHI Regulations (e.g. heating empty buildings or empty greenhouses, using inappropriately sourced fuel), or may waste heat in a compliant manner by using heat in a non-energy efficient way.**

- **Over sizing of boilers to ensure high proportion of heat is generated at a higher tariff rate; under sizing of boilers/installing multiple separate boilers in order to maximise the applicable tariff rate.**

  Prevention: To help combat this, the RHI Regulations stipulate what constitutes eligible heat and give Ofgem the power to ask participants for evidence to demonstrate that the heat they are claiming RHI for is being used for eligible purposes. The Regulations also clearly state that participants should not generate heat purely for the purpose of increasing RHI payments. In addition, the tiered tariff for biomass (meaning a higher tariff rate is paid for the first 15% of annual heat generation hours) reduces the incentive to purposefully generate then waste heat.

  At present no remedy is available within the RHI regulations to address the issue of over/under sizing of boilers. Information has been provided to DECC and consideration is being given to regulatory amendments.

8. Detection

8.1 Despite the mitigating actions put in place, there will be instances when fraud or non-compliance will occur. In order to combat this, we have a range of mechanisms in place to enable us to identify fraud or non-compliance and deal with it as soon as possible. These include:

i. A rolling programme of on-site audits of accredited and pre-accredited installations. Installations will be subject to inspection both at the accreditation stage and throughout the duration of eligibility for incentive payments. In accordance with the RHI site audit plan, site audits will take place regularly throughout the year and, as mentioned above, will consist up of a mix of targeted and randomly selected installations. We have an Audit Strategy for audit of RHI installations and this is due to be reviewed in the new year.

ii. In addition to site inspections, we carry out desk-based audits, which includes review of relevant documentation.

iii. Robust IT monitoring, reporting and quality management systems: in addition to standard security features, various checks are built into the RHI IT system such as

- Tolerance level checks (to help identify cases where there may be anomalies in data submitted)
- Suspicious item matching (e.g. Matching post codes, serial numbers etc)
- Functionality to identify cases for targeted inspections (eg. where the declared heat output is slightly within tariff thresholds, multiple installations on one site etc.)

iv. Watch lists for staff to record concerns about installations, periodic data or IRMA providers.

v. Ofgem whsitleblowing procedure for members of staff and the public to report any concerns to us

vi. Ofgem fraud policy that sets out staff responsibilities with regard to fraud prevention and includes the procedure for staff to report any fraud or suspicions of fraud

vii. Sharing and exchanging information with other government departments as appropriate. This is subject to any legal requirements and Ofgem's own policies/procedures regarding the exchange of information. Ofgem will only exchange personal data in accordance with the requirements of the Data Protection Act 1988[4].

viii. All operational members of the NDRHI team complete mandatory e-learning training on Fraud Prevention and Whistleblowing. This increases staff awareness and knowledge of fraud prevention and detection and encourages staff to pro-actively identify fraud risks. In addition, the NDRI Fraud and Compliance Team deliver training sessions to staff as required and provide feedback on findings. This will help to ensure that staff are more aware and alert to triggers and what they should look out for.

ix. Our Internal Auditor (Deloitte) has a key role in designing and carrying out tests to detect fraud and highlight weaknesses in the NDRHI administration process to ensure that it is as fraud proof as possible.

9. Handling identified instances of suspected fraud

9.1 Any suspected fraudulent or non-compliant activity in relation to the NDRHI scheme should be reported to the Fraud and Compliance Manager who will decide how to conduct an investigation. They may need to be guided by the Fraud Prevention, Audit and Governance Team, NDRHI operational and technical staff, and/or legal staff in reaching this decision.

9.2 The Fraud and Compliance Manager will ensure that an Instant Notification Report (INR) is circulated to appropriate staff.

9.3 Ofgem E-Serve's Fraud Policy (FRM04/2012) should be followed when securing evidence in an investigation.

[4] www.legislation.gov.uk/ukpga/1998/29/contents

10. Review of decisions

10.1 As stated at paragraph 5, for cases where we establish non-compliance with the scheme, we may enforce one or more of the range of sanctions that are available to us under the Regulations.

10.2 Where we do impose a sanction on a participant, we will

- Inform the person or business concerned why we have taken the decision
- Provide details of evidence supporting the decision
- Outline the effect of the decision
- Outline the review process available including steps the participant must take to instigate the review.

10.3 Where a review takes place, the outcome could be to

- Confirm the sanction
- Amend the sanction or replace it with one or more alternative sanctions
- Remove the sanction

11. Next Steps

11.1 Ofgem remain committed to addressing the fraud risks within the NDRHI scheme We will constantly continue to review and revise this strategy to ensure it remains relevant, fit for purpose and continues to provide assurance on the level of fraud prevention activity that is in place for the NDRHI.

11.2 Discussions are underway with the legal team and DECC as part of a review of the effectiveness of the current sanctions regime.

12. Conclusion

12.1 We are committed to tackling fraud and non-compliance within the RHI and we will work hard to ensure we do this in an effective and organised way including liaising closely with other schemes within Ofgem and will rely on the principles included in this document to achieve this.

12.2 We will continue to review our rules and procedures and will make sure that this document is reviewed at least annually to ensure that it remains effective.

13. References

13.1 Ofgem IT Security Policy (link to IT security policy)

13.2 Ofgem Fraud Policy (link to Ofgem fraud policy)

13.3 Ofgem Whistleblowing Policy (link to Ofgem internal whistleblowing policy)

13.4 Fraud Risk Register (link to NDRHI fraud risk register)

14. Version History

Version	Date	Author	Comment
1	February 2011	Ade Obaye	First draft
2	March 2011	Ade Obaye	Presented to the RHI Implementation Board
3	31 October 2011	Ade Obaye	Final update before scheme launch
4	20 August 2012	Paul Heigl	Updated to include Northern Ireland RHI
5	4 December 2013	Ade Obaye	Reviewed and updated to add further detail