ofgem e-serve Policy/Guidance

NDRHI Fraud Prevention Strategy for Northern Ireland

This document outlines the strategy and processes for identifying, controlling and mitigating the risk of fraud within the NI Non-Domestic RHI schemes. It also sets out the process for managing suspected fraud cases within the scheme.

Author	Sharon Fyfe, Counter Fraud Manager
Audience	Gareth John, Teri Clifton, Edmund Ward, Counter Fraud Team
Date policy first issued	December 2016
Date policy reviewed	n/a

Contents

1. Version History

Ver	Date	Author	Comment
0.1	December 2016	Sharon Fyfe	First Draft

2. Introduction

2.1. The Non-Domestic Renewable Heat Incentive (NDRHI) is a scheme introduced by the Northern Irish Government which is designed to promote the uptake of renewable heat generation technologies within the non-domestic sector.

2.2. Now that the NI scheme is currently closed to new applicants, a separate fraud policy has been devised to focus on detection and monitoring of ongoing compliance.

- The NDRHI is administered by Ofgem E-Serve on behalf of the Gas and Electricity Markets Authority (GEMA) for the Department for the Economy (DfE) in Northern Ireland. The NI scheme was suspended for new applicants on 29th February 2016, therefore our current role as administrator of the scheme includes responsibility for:
  - Making payments to participants for eligible heat produced;
  - Monitoring and enforcing compliance with the on-going requirements of the

scheme;
- Undertaking inspections to ensure participants are compliant with on-going obligations.

2.3. A key aspect of the administration of NDRHI is a robust, effective and proportionate fraud prevention framework. This document describes the strategy for mitigating the risk of fraud and providing fraud prevention support, advice and information to the Northern Ireland NDRHI team.

2.4. In developing this strategy we took into account the scheme's budget and what's proportionate in the context of the scheme when determining effective solutions for mitigating fraud risks.

3. Scope and limitations of the NDRHI Fraud Prevention Strategy

3.1. If the scheme is re-opened to new applicants, the Fraud Prevention Strategy will be reviewed to take account of the application process as this document now focuses on existing scheme participants only.

3.2. This strategy is based on information which we are aware of at the time of drafting. It is an evolving document which is refreshed periodically as the scheme matures, as individual directorate counter fraud plans are agreed and as new risks emerge.

3.3. It is important that the risk management processes in place in Ofgem E-Serve capture fraud risks and allow us to monitor and mitigate them effectively.

3.4. We are aware that, as with many schemes, the design may allow 'gaming' opportunities. It is important to note that such occurrences are not considered to be fraud as they are not in breach of the Regulations. However if we become aware of gaming activity, we will report it to the NI NDRHI Policy team so they can make DfE aware of areas where a legislative amendment might be considered.

3.5. There is a financial and reputational risk upon Ofgem E-Serve in relation to the risk of external fraud from scheme participants and industry third parties.

3.6. The nature of the Northern Ireland NDRHI scheme means that there may be a number of parties involved when the application was accredited, including the applicant, installer and consultant. However, Ofgem's relationship is with the scheme participant and we have no enforcement powers against those involved in this supply chain.

3.7. If suspected fraudulent activity is found which leads to the participant breaching the eligibility requirements and/or ongoing obligations outlined in the NDRHI Regulations, we may make recommendations to the Compliance teams to apply an appropriate sanction available under the regulations.

3.8. It is important to note that on the NI NDRHI scheme there is a referral filter in place at Delegated Authority level. This means that when a member of the NDRHI scheme team has a suspected fraud concern they must route it through another member of the team with Delegated Authority for review before a decision is made as to whether to pass the concern to the Counter Fraud team.

3.9. Ofgem has no statutory power to investigate fraud (defined in section 4). This means that our role is limited to gathering information with the aim of substantiating allegations in circumstances where fraud may be suspected. We are also responsible for referring cases to the relevant police authority or Action Fraud.

4. Definition of Fraud

4.1. For the purpose of this document, fraud is as defined in the Ofgem Fraud Policy (FRM04/2012)

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

4.2. Therefore, for a fraud to occur the person must have acted dishonestly **and** acted with the intent of making a gain for themselves or someone else, or inflicting a loss (or risk of loss) on another.

4.3. In the context of NI NDRHI, fraudulent activity is regarded as covering any dishonesty in relation to the NDRHI Regulations and/or Guidance that would have the effect of causing a loss (or risk of loss), or securing a gain for someone. It does not necessarily have to be a financial loss for Ofgem, or a financial loss at all. Only that there was intent to make a gain or cause a loss.

4.4. For an act to be considered possibly fraudulent as opposed to non-compliant there must be a suggestion that there was 'intent' by the party in question. On Cabinet Office advice, the level of evidence which must be obtained to demonstrate fraudulent activity is based on **the balance of probabilities**. This is the civil level of proof, as opposed to the criminal level of proof (beyond reasonable doubt).

5. Fraud Threats

5.1. Below are the main sources of fraud threats, both internal and external, to the NDRHI scheme:

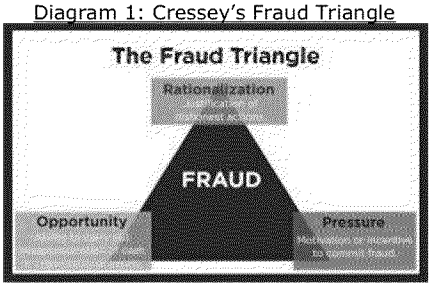
Internal Fraud Threats

5.2. Staff within Ofgem (including temporary and permanent staff, current and previous) could commit internal fraud by:

- Stealing, or using inappropriately, personal data held on scheme computer systems or held in hard copy form (e.g. bank details);
- Colluding with a scheme participants to bypass controls or to manipulate data submissions;
- Fraudulently changing participant details to increase payments;
- Diverting payments to alternative bank accounts;
- Changing details on existing accreditations to allow payments to be made into their own bank account.

5.3. Cressy's Fraud Triangle (Diagram 1) explains the 3 motivating factors for committing internal fraud and our focus is primarily on reducing the opportunity for internal fraud. The employee committing the fraud usually sees an internal control weakness and, believing no one will notice, begins the fraud on a small scale. If no one notices, the level of fraud will usually increase.

Diagram 1: Cressey's Fraud Triangle



In any organisation, the risk of fraud can be reduced. Internal control procedures can particularly diminish the "opportunity" point of the Fraud Triangle. Within NI NDRHI, controls have been put in place to reduce the opportunity, e.g. by restricting staff that have access to bank and ID information.

There is a 'zero tolerance culture' embedded through mandatory E-Serve and scheme specific fraud awareness training, as well as whistleblowing awareness training.

External Fraud Threats

- Participants could provide false meter readings or periodic data in order to increase the level of NDRHI support payments they receive;
- Participants may not have informed us that they have sold their business and still continue to claim payments for which they are no longer entitled to.
- Participants could collude with a third party to provide false information to Ofgem to gain payments to which they aren't entitled i.e. site inspection auditors.
- Participants could falsely claim in their annual declaration that they are still entitled to Non Domestic payments but their status has changed and they are no longer eligible for payments.
- False information is provided in relation to change of use, in order to game the amount of eligible heat output.
- For cases which are yet to be accredited, applicants may provide false information as part of their application, e.g. date of finstallation.

5.4. To effectively mitigate against these risks, the Counter Fraud team reviews the scheme fraud risks on a quarterly basis. The purpose of these reviews is to:

- Identify new and emerging fraud risks and add these to the NI NDRHI risk register with an appropriate risk owner;
- Ensure that all fraud risks have been assessed appropriately in relation to their anticipated likelihood and impact or, if the circumstances have changed since the risk was added/updated, amended as necessary;
- Identify possible mitigating controls and actions and determine if these are proportionate to the risk;
- Ensure that all actions are being progressed by the appropriate action owner;
- Review the effectiveness of mitigating controls already in place;
- Identify any risks which have expired and should be closed off.

6. Sampling/Assurance

6.1. The use of sampling is widely adopted because it offers the opportunity for the 'auditor' to obtain the minimum amount of audit evidence, which is both sufficient and appropriate, in order to form valid conclusions on the total number of accreditations.

6.2. In devising the samples, the Counter Fraud team will ensure that the sample selected is representative of all accreditations, to ensure valid conclusions can be made.

6.3. The Counter Fraud Team agrees to complete sample checks on a yearly basis on the NI NDRHI scheme. This will be in addition to the annual site audit programme. Checks will include the following, however we will review this regularly to ensure that is based on current fraud risks.

- Conducting additional checks in relation to the annual declarations, to ensure they are still compliant with the regulations and entitled to payments. This may include open source research (e.g. company websites, Companies House, Zoopla), alongside contacting participants for further verification.
- Conducting additional checks in relation to change of ownership cases to ensure they are still compliant with the regulations and entitled to payments. As above, this may include open source research or may require us to write to participants for additional evidence.
- Desk top audits on accredited cases to review company status. This may involve Companies House checks or requesting current evidence of non-domestic status from the applicants.
- Review of Periodic Data payments on a quarterly basis to complete trends analysis and review any anomalies. We will establish the norm perameters of heat use and analyise outliers.
- Reviewing amendments related to change of heat use to identify instances of potential abuse of the scheme (e.g. increased heat usage).

6.4. The Counter Fraud team will split the sample so that 50% of the checks are targeted (based on high risk indicators, e.g. those participants who are receiving unusually high payments) and 50% of the sample is randomly selected.

6.5. If there are areas of high concern then we may change the selection strategy to a risk based sampling strategy for all our checks.

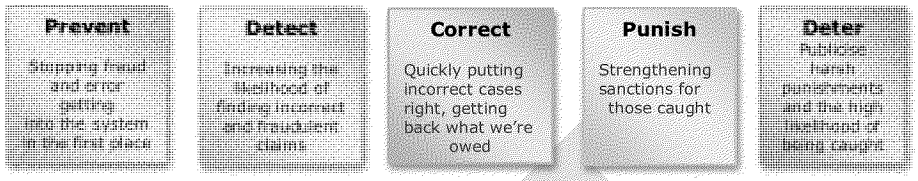
Comment [ST1]: Discussed internally an we are working on a model of 3% per year, however this will be agreed as par of the conversations with DfE.

Comment [ST2]: Edmund- does this see reasonable in relation to the NI NDRHI audit strategy?

7. NI NDRHI Strategic Approach to Fraud Risk

7.1. The Fraud, Error and Debt team within the Cabinet Office promotes **5 principles** to tackling fraud and error (illustrated below). We have adapted and aligned our strategy to these principles and set out below how we will practically attain each of these in the context of NI NDRHI.

5 Principles to tackling Fraud and Error



NI NDRHI Fraud Prevention Strategy

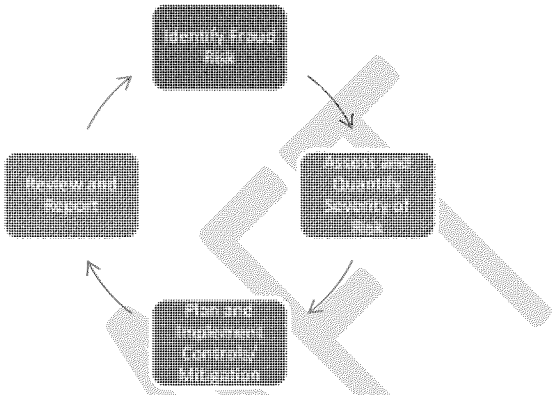
Prevent	Detect	Correct	Punish	Deter
Implementing lessons learned from suspected fraud Investigations. Regular review and refresh of key fraud risks. Staff awareness training on fraud awareness and key fraud controls. Implementation of Ofgem's Fraud Policy. Intelligence sharing with DfE on cases of suspected fraud. Jane/ Edmund- this will link in with the revised administration arrangements Staff currently undergo checks through Disclosure Scotland and CIFAS. Ongoing fraud awareness training for exisiting staff.	Programme of site audits post accreditation, as set out in NI NDRHI Audit Strategy. Percentage check on annual declarations. Counter Fraud sampling checks. Rigorous amendment review process. Implementation of Ofgem's internal/ external Whistleblowing Policies. Counter Fraud hotline and inbox for members of the public to report suspected fraud matters directly to us. Use of data analytics. Review of PD payments on a quarterly basis.	Clear ownership of suspected fraud investigations process. Process for referring cases to Compliance and Audit teams if suspected fraud not established but potential non-compliance is identified. Clear reporting process for suspected fraud to DfE via the monthly performance pack. Feedback mechanisms to rectify issues identified, particularly where they are systemic (e.g. feedback to DfE through Policy Team). Trend analysis of suspected fraud referrals.	Referral to NI law enforcement agencies and Action Fraud. In the case of suspected non-compliance, sanctions are available as outlined in the NI NDRHI legislation, for example: -Suspend periodic support payments either temporarily or permanently; -Revoke accreditation or registration; -Recoup overpaid periodic support payments. *Teri as discussed	The NI NDRHI Guidance sets out a zero tolerance approach to fraud. It's also made clear that sanctions can be imposed. Regular comms on twitter, etc to make people aware of their ongoing commitments and the Counter Fraud Team. Check with Stuart, does this reach NI? The threat of payments being suspended whilst an investigation is undertaken. Counter Fraud webpage sets out our zero tolerance policy to fraud. Check this is on DfE website

8. Prevention

Robust Risk Management Framework

8.1. The NI NDRHI scheme seeks to gain assurance on fraud risks through the application of a range of tools to monitor the risk and control environment. This is achieved through implementation of robust risk management process as part of the day-to-day operation of the NI NDRHI scheme.

The diagram below sets out the basic risk management process for all E-Serve Schemes.



It is the responsibility of NI NDRHI Senior Management to ensure risk management procedures are embedded across the scheme. Counter Fraud staff are actively engaged in this process and recommend the inclusion of emerging fraud risks and/or changes to identified fraud risks within the scheme risk register, as well as possible mitigating controls.

Risks are managed in line with the E-Serve Risk Management Framework.

Fraud Risk Recording and Reporting

8.2. The fraud risks on the NI NDRHI scheme are captured within the Scheme Risk Register. Counter Fraud Managers review these risks on a monthly basis and attend the scheme's monthly risk review meetings, where severity of risks and status of controls are discussed as well as new risks and risk closures.

8.3. Current scheme highest risks are shared with the E-Serve Risk and Fraud Management Group every two months, through the E-Serve Schemes Highest Risks Register. If necessary, the group can decide to escalate a risk to the E-Serve Top Risks Register or amend an existing risk.

8.4. On the NI NDRHI scheme, fraud risks are owned by a representative from that scheme rather than a Counter Fraud Manager. This means that the scheme representative is ultimately responsible for ensuring that controls are implemented and working effectively.

Sharing Best Practice

8.5. Counter Fraud staff with responsibility for NI NDRHI work with Counter Fraud colleagues on other schemes to share best practice, utilising the knowledge and expertise of other teams to identify potential fraud controls, mitigation and process improvements.

Control Environment

8.6. During the development of the scheme, controls were put in place to prevent and detect fraud against the scheme. It's essential that new or revised Standard Operating Procedures (SOPs) are reviewed by the Counter Fraud team in order to ensure that controls remain adequate to mitigate the risk of fraud.

8.7. All amendments to the NI NDRHI are thoroughly reviewed to ensure installations meet the eligibility requirements for the scheme. If the amendment reviewer notices something in the application which they suspect may be fraudulent, the matter is referred to a Delegated Authority for consideration. They will then determine whether the matter should be referred to Counter Fraud for investigation. The Counter Fraud team explores each concern and engages the NI NDRHI Operational team where necessary. One of the aims of this step is to stop potentially fraudulent amendments being approved.

8.8. A further control in place is the Bank and ID verification at amendment stage through a third party provider, if changes are made to the owner.

8.9. Ofgem has a zero tolerance approach to internal fraud. Protections against internal fraud include an organisation-wide fraud policy, internal and external whistleblowing policies and an employee Code of Conduct. Disclosure Scotland and CIFAS checks are also carried out on all staff when they are appointed.

8.10. All members of the NI NDRHI team complete mandatory e-learning training on fraud prevention and whistleblowing. Staff are also required to undertake Protecting Information e-learning, Information Rights training, and Information Security training. This increases staff awareness and knowledge of fraud prevention and detection and encourages staff to proactively identify fraud risks and report possible instances of fraud to Delegated Authority.

9. Detection

9.1. Despite the mitigating actions put in place, there may be instances when fraud occurs on the NI NDRHI scheme and as such, we have a number of mechanisms in place to identify and act against it.

Audit Strategy

9.2. We have a programme of on-site audits of accredited installations in place. Site audits take place on a rolling basis throughout the year and consist of a mix of targeted and randomly selected installations. Suggestions for site audits can be made by the Counter Fraud team and can be used to support the investigation of allegations of suspected fraud.

9.3. The NI NDRHI Audit Strategy is developed and maintained by the Audit team.

9.4. Sampling checks will take place by the Counter Fraud Team (as outlined in section 6) to review aspects of the process in addition to the Audit Strategy.

IT Systems

9.5. Robust IT monitoring systems are in place as part of the NI NDRHI IT systems, such as:

- Tolerance level checks (to help identify cases where there may be anomalies in data submitted), for example to ensure that reported heat generation is feasible in relation to system capacity;
- Data cross-matching (e.g. matching postcodes, duplicate serial numbers etc.);
- Functionality to identify cases for targeted audits (e.g. where declared heat output is just within tariff thresholds, multiple installations on one site etc.).

Policies and Reporting of Concerns

9.6. Ofgem whistleblowing processes for staff/public to report concerns to us;

9.7. 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;

9.8. Members of staff are able to report suspected fraud by discussing their concern with a Delegated Authority on the scheme. The Delegated Authority will determine whether the matter should be referred to Counter Fraud. If they decide it should, the member of staff can contact the Counter Fraud team either by emailing the Counter Fraud inbox (counterfraud@ofgem.gov.uk) or by speaking to a member of the Counter Fraud team directly, either face to face or by telephone.

9.9. A Counter Fraud telephone hotline is available for members of the public to report suspected fraud matters directly to us.

Data Analytics

9.10. The Counter Fraud team has implemented Qlikview data analytics which allows us to interrogate NI NDRHI data more effectively. This allows the Counter Fraud team to scrutinise suspicious accredited installations in a more effective way.

10. Correct

10.1. Any suspected fraudulent activity in relation to the scheme should be reported to the Counter Fraud team. The nominated Counter Fraud Manager or Assistant Manager will objectively assess the information received to determine whether the issue is a matter of suspected fraud. This will be based on experience and knowledge of the scheme.

10.2. At times, we may require further information in order to make our assessment. In these instances we may request information from the original referral source, scheme participant or via site audit, where appropriate. Guidance may also be sought from the Head of Counter Fraud, Associate Director, Heads for Non-Domestic RHI and/or Ofgem Legal staff in reaching this decision. Further information may also be sought from the NI NDRHI Operational, Audit, Compliance or Technical teams.

10.3. Where instances of suspected fraud are identified, these will be registered by the Counter Fraud team and recorded in the suspected fraud database. A report detailing all new and closed cases of suspected fraud on the scheme is prepared fortnightly and shared with key internal stakeholders (including scheme Associate Director and scheme Heads).

Comment [ST3]: Do we want to share w DfE under new admin arrangement?

10.4. The high level process for investigating suspected fraud cases is set out within the Counter Fraud Team Manual.

11. Punish

Applying Sanctions

11.1. Ofgem has a range of sanctions available that can be applied. Where there is sufficient evidence of non-compliance or fraudulent activity which has resulted in a breach of regulations, such sanctions may be applied. Counter Fraud will provide information and recommendations to scheme Delegated Authority colleagues on suspected fraud matters, evidential bar and possible sanctions. Scheme Delegated Authority will then make the decision and apply sanctions.

11.2. Some of the key sanctions available are:

- Power to withhold periodic support payments to investigate alleged non-compliance
- Power to withhold periodic support payments where there is a failure to comply
- Power to permanently withhold or reduce periodic support payments
- Revocation of accreditation

Referrals to Law Enforcement/Action Fraud

11.3. Following investigation, if we determine that there is enough evidence to substantiate our suspicions of fraud we will refer the matter directly to Action Fraud, where a decision will be taken as to whether criminal proceedings will be instigated. We will seek feedback from Action Fraud on whether the matter has been taken up by an authority such as the Police and will cooperate in any investigations.

12. Deter

12.1. One of the main deterrents against external fraud threats involves highlighting the consequences of fraud within key information and guidance available to scheme participants.

12.2. Additionally scheme applicants are asked to sign a declaration confirming that all information in their application is true to the best of their knowledge. They are required to renew this declaration on an annual basis as part of their ongoing obligation.

13. Stakeholders/ Agencies

The main stakeholders/agencies currently associated with the Northern Ireland NDRHI fraud prevention are:

- NI NDRHI Team
  Has responsibility for the day-to-day running of the scheme and acts as the first line of defence. This includes, but is not limited to, the Periodic Data, Amendments, Audit, Compliance and Technical teams.
- NI NDRHI Scheme Board
  Receives monthly updates on scheme activity, including high level summary of suspected fraud cases and work undertaken by the Counter Fraud team.

- E-Serve Risk and Fraud Management Group (RFMG)
  Has the authority to scrutinise and challenge the activities undertaken by E-Serve to minimise the risk of fraud in connection with E-Serve schemes. RFMG also has oversight of risk management activities in E-Serve.

- E-Serve Counter Fraud Team
  Shares best practice for the prevention, identification and escalation of fraud within Ofgem E-Serve schemes. The team also carries our peer review and challenge of scheme fraud risk registers and fraud prevention strategies and investigates allegations of suspected fraud.

- Department for Economy (DfE):
  Ofgem monitors the Northern Ireland NDRHI scheme on behalf of DfE.

- Action Fraud
  Provides a function for Ofgem to report suspected fraud.

14. Year Ahead

14.1. Ofgem remains committed to addressing the fraud risks within the NI NDRHI scheme. The processes identified above are regularly reviewed to ensure the fraud prevention strategy remains fit for purpose and effective in achieving its aims.

14.2. Representatives from the NI NDRHI scheme have been consulted in relation to the focus of Counter Fraud activity and a new strategy session will be set up for the start of February 2017 to discuss the focus for the year ahead.

15. References/ Additional Information

15.1. Ofgem Fraud Policy (FRM04/2012)

15.2. Ofgem Whistleblowing microsite

15.3. Ofgem website for most up to date guidance and Regulation documents

15.4. NI NDRHI Risk Register