RETAIL ENERGY CODE

ENERGY THEFT TRAINING

MODULE THREE –
DESKTOP INVESTIGATION AND DATA GATHERING

ENERGY THEFT DESKTOP INVESTIGATION

RETAIL ENERGY CODE

The purpose of an Energy Theft Desktop Investigation is to:



Assess and substantiate an Energy Theft lead, gathering relevant information to determine whether there is enough suspicion or evidence to justify further investigation. Outcomes may include:

- No further action
- A site visit
- Continued monitoring and a later desktop review when more data becomes available



Collect and document additional useful information in preparation for any subsequent Energy Theft Site Visit Investigation, including:

- Health and safety risks
- Consumer vulnerabilities
- Any previous Energy Theft history

DEFINING THE DESKTOP INVESTIGATION

Energy Theft Desktop Investigation is a **defined term** in REC Schedule 1.

The definition details the minimum requirements that must be evidenced to qualify for the relevant Theft Detection Inventive Scheme (TDIS) payments detailed by the Theft Target Methodology.

The definition is structured with an introductory paragraph followed by eight detailed sections (a–h), which are explored in the following slides.

Take care to document!

Consider how to **document your desktop reviews** to evidence requirements have been met. Whether you use specialised software *(recommended where investigations are conducted at volume)* or another approach, you will need to be able to report on the outcomes for your TDIS submissions.

Prepare to send

If it's determined that the investigation needs to progress, you'll need to be able to **pass the information** collated to the person who will be conducting an **Energy Theft Site Visit Investigation.**

THE DEFINITION

RETAIL ENERGY CODE

REC Schedule 1

Energy Theft Desktop Investigation

means that the holder of an Energy Licence (or person acting on their behalf) conducts a desktop investigation to determine the potential likelihood of Energy Theft and requirements of further investigation. **As a minimum the desktop investigation must include and evidence**:

…

REQUIRED INCLUSIONS

RETAIL ENERGY CODE

- (a) the source, date and details of the initial report of suspicion of Energy Theft
- (b) the date of the desktop investigation and the name/ID of the person who conducted it. If the desktop investigation was fully or partly automated this should be recorded with the automation process made available on request
- (c) if the potential Energy Theft is being investigated by or on behalf of an Energy Supplier, that the Energy Supplier is the current Registered Supplier at the time of the investigation (in which case the Supply Effective From Date and any known Supply Effective Through Date shall be recorded)
- (d) the relevant Consumer's name, address and MPAN/MPRN, and the dates of the last Change of Occupier and any known future Change of Occupier
- (e) any correspondence or contact with the Consumer or a third party concerning the potential Energy Theft
- (f) review of meter details, any metering work, meter readings, consumption, alerts and payment activity relevant to the investigation
- (g) any previous known theft investigations at the premises or linked to the Consumer
- (h) a determination that the suspicion of Energy Theft is invalid, and the investigation may be closed; or that the suspicion of Energy Theft is valid and should progress to an Energy Theft Site Visit Investigation.

(A) THE SOURCE AND INITIAL REPORT

RETAIL ENERGY CODE

(a) the source, date and details of the initial report of suspicion of Energy Theft

Understanding where the lead originated helps establish its **credibility**.

HIGHLY CREDIBLE	CREDIBLE BUT VARIABLE DETAIL	DATA-DRIVEN LEADS
Reports from trained meter operatives who have visually identified evidence.	Information from ETTOS, members of the public, or other informal reporters	System-flagged anomalies suggesting possible theft. Require further investigation but remain important.

It is important to accurately record and document **when and how** the lead was reported, as well as the information provided as it forms part of the evidence.

Did you know? CrimeStoppers.

If a Crimestoppers report is flagged as **Online (two-way)**, the anonymous reporter has chosen to remain **contactable**. Investigators can request more details by emailing **cis@treblefive.co.uk**. This communication window lasts 14 days from the report date and can provide crucial additional information.

(B) WHO AND WHEN

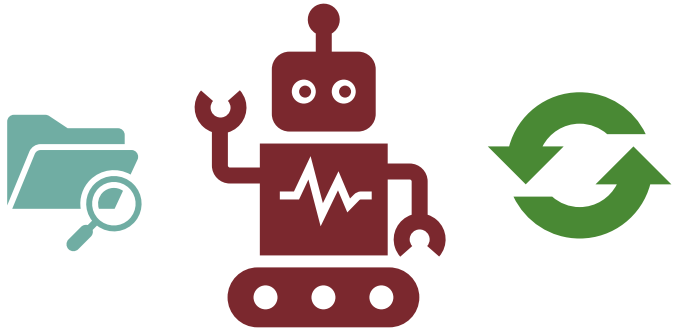
RETAIL ENERGY CODE

(b) the date of the desktop investigation and the name/ID of the person who conducted it. If the desktop investigation was fully or partly automated this should be recorded with the automation process made available on request

You must record **who carried out** each Energy Theft Desktop Investigation and the date it was completed.

If any part of the investigation is automated, you must record whether automation was used **instead of** or in **addition to** manual investigation. Any automation used must be:

Fully documented, including the data sources and rules it relies on.



Repeatable, so that the same process can be followed consistently.

This documentation may be reviewed during performance assurance activities, so it must be **accessible and complete**.

(C) THE REGISTERED SUPPLIER

RETAIL ENERGY CODE

(c) if the potential Energy Theft is being investigated by or on behalf of an Energy Supplier, that the Energy Supplier is the current Registered Supplier at the time of the investigation (in which case the Supply Effective From Date and any known Supply Effective Through Date shall be recorded)

You must first confirm that your organisation is the current electricity or gas Supplier for the meter point, and you therefore are authorised to carry out the investigation. **You are only authorised to investigate meter points you currently supply.**

Check the **Electricity Enquiry Service (EES)** and **Gas Enquiry Service (GES)** to confirm and record the supply start date.



Important! If the consumer switches Supplier during your investigation, **you must close the investigation** using the TDIS Current Investigation (Code L – No Longer Supplied). As required by REC Schedule 8, the outgoing Supplier must notify the incoming Supplier that an investigation was in progress. This can be done on the Secure Data Exchange Portal (SDEP) using Market Messages: **PT0075** – Theft General Query (Electricity) | **PT0074** – Theft General Query (Gas)

If the lead relates to electricity, it is helpful to determine if the premises has a gas supply, regardless if you are the gas supplier or not. Reviewing both accounts provides a fuller picture for the desktop investigation. If you have only recently gained the supply, check whether you have supplied the premises previously and review historic account information where available.

(D) THE ADDRESS AND THE OCCUPIER

(d) the relevant Consumer's name, address and MPAN/MPRN, and the dates of the last Change of Occupier and any known future Change of Occupier

When verifying the address and MPxN details during a desktop investigation:



Verify the address and MPxN using GES, EES, and your own account management systems. If unclear, use tools such as Royal Mail postcode finder or Google Maps. If uncertainty remains, record the concerns as part of the investigation.



If you don't supply the premises, **pass the information to the Registered Supplier** or (if no Supplier can be identified) the relevant Network Operator.



Confirm account holder details and record if they match or differ from those provided in the initial report. Additional verification tools that could be useful include Credit reference agencies, Land Registry and Companies House.



Review change of occupier history and record previous and future Change of Occupier (CoO) events.

Consider **how any occupancy change was notified** and who notified it. This helps determine who may be responsible for the theft and whether the current occupier inherited the tamper.

(E) CORRESPONDENCE AND CONTACT

RETAIL ENERGY CODE

(e) any correspondence or contact with the Consumer or a third party concerning the potential Energy Theft



As part of a desktop investigation, **review all forms of correspondence and customer contact** linked to the account to understand their relevance to the initial suspicion of theft.

- Check for **letters, emails, texts, or online messages** associated with the Consumer or account.
- **Check phone call logs**: who called, what did they claim, does the phone number match the account?
- Consider how correspondence may **relate to the initial report**.
- Consider whether the Consumer may be attempting to **mislead or obstruct detection**.
- Consider whether **recordings exist and could be used as evidence**.



Such correspondence may not directly identify theft but can provide useful information including around access and landlord details, Consumer vulnerability or on expected consumption patterns.

(F) METER DETAILS, ALERTS AND PAYMENTS

RETAIL ENERGY CODE

(f) review of meter details, any metering work, meter readings, consumption, alerts and payment activity relevant to the investigation

Verify Meter Details and History

- Review your internal account management systems and GES/EES data to confirm **meter serial number**, **type**, **installation date**, and **payment mode**.
- Check **records of metering work**. Have engineers accessed the property? Was their work successful?
- Identify when the meter was **last inspected and confirmed to be functioning** without interference (trickier if meter pre-dates supply).

Assess Meter Readings and Consumption

- Identify what **readings** you hold (actual, smart, customer-supplied, or estimated).
- **Compare billed/recorded consumption against expected usage** developed during the desktop review. Customer or estimated readings may be unreliable.

Smart Meter Behaviour and Alerts (if applicable)

- Check if the **smart meter is communicating** correctly; communication failures may indicate tampering.
- **Review any alerts** generated, timing, and how they align with recorded consumption patterns.



(F) METER DETAILS, ALERTS AND PAYMENTS CONT.

(f) review of meter details, any metering work, meter readings, consumption, alerts and payment activity relevant to the investigation

Fuel Comparison

- Compare **consumption across gas and electricity** if you supply both.
- Identify unusual patterns (e.g. gas normal but electricity near zero) which may indicate tampering.

Property Characteristics

- Identify property type (domestic/commercial), size, occupancy, landlord/owner details, and if commercial, check the business type and opening hours.
- Check publicly available licensing or food hygiene information, linked business sites, or planning applications via the Local Planning Authority.

Billing and Payment Behaviour

- Review **whether the customer pays their bills**, how they pay
- Has there been any changes, if so when and how does this relate to the initial report, consumption patterns or alerts e.g.
  - They previously struggled with high-usage payment plans and then a sudden drop in consumption.
  - Pre-payment meter top ups stopped and terminal cover removed alert around the same time.
- After debt disconnection, advancing meter reads or indications of power use may indicate illegal reconnection.



(G) PREVIOUS ENERGY THEFT INVESTIGATIONS

RETAIL ENERGY CODE

(g) any previous known theft investigations at the premises or linked to the Consumer

- Has any **previous Energy Theft Site Visit Investigations or Energy Theft Desktop Investigations** taken place, and what were the outcomes?
- Was it the **same Consumer or a previous occupier**?
- Do you have any records of investigations linked to the **same Consumer but at a different address**?
- If it didn't precede beyond desktop investigation previously, is the reasoning still the same or is there now **additional reason to suspect theft**?
- If there was an Energy Theft Site Visit Investigation before and they did not find theft, what was the explanation and what has or may have changed since the visit?
- If the meter was found to be faulty, does it appear to be faulty again? Is there a **suspicion that it has been tampered with** to appear faulty?







The history of theft investigations should be taken into consideration when deciding whether to progress. It is important that this information is documented for the investigator who will be attending site.

(H) MAKING A DETERMINATION

(h) a determination that the suspicion of Energy Theft is invalid, and the investigation may be closed; or that the suspicion of Energy Theft is valid and should progress to an Energy Theft Site Visit Investigation.

- All information gathered should be considered when determining **whether to progress to an Energy Theft Site Visit investigation** or to close the investigation as “No Theft”.
- Consider if you can substantiate the details of the initial report (or rule them out). Is there a possibility of theft, does an **Energy Theft Site Visit Investigation** need to take place to find out or is there strong evidence that theft is occurring so a site visit must take place to resolve it and any safety concerns?
- You may choose to have the desktop investigation **remain open** for a period to gather further information or monitor the account. If this requires a longer period of monitoring it may be beneficial to close as invalid as currently insufficient information to progress and then initiate a future desktop investigation once additional information is available.
- Your **criteria for determining** to progress or close an investigation should be detailed in your **company’s policy and processes**.



Whilst you must make a judgement as to the likelihood of theft occurring – and you can decide that it is not appropriate to progress based on information available – remember that you can **never truly rule out Energy Theft by a desktop review alone**.

RETAIL ENERGY CODE

KNOWLEDGE CHECK

KNOWLEDGE CHECK

RETAIL ENERGY CODE

Congratulations, you have completed Module 3!

Please complete the Knowledge Check to ensure you have understood the key messages from this module.

