RETAIL ENERGY CODE

ENERGY THEFT TRAINING

MODULE TWO –

REACTIVE AND PROACTIVE ENERGY THEFT LEADS

WHAT IS AN ENERGY THEFT LEAD?

RETAIL ENERGY CODE

An **Energy Theft Lead** is any information, intelligence or evidence that indicates Energy Theft may be occurring.

This could include: **physical signs** 

something that has been **overheard or said** 

data that is **collected and analysed** 

Leads fall into two categories:

Reactive (Tip-Offs)	Proactive (Data Driven)
Reports from individuals or organisations based on what they've **seen, heard, or know**.	Identified through **data analysis**, using manual checks or automated methods like algorithms, machine learning, or AI to **detect anomalies** indicating possible theft.

REACTIVE ENERGY THEFT LEADS

RETAIL ENERGY CODE





A reactive lead could come from an **industry expert**. Schedule 8 section 6 and Schedule 14 along with CoMCoP details the obligation to pass these leads on.

This could be, for instance, an employee or contractor of an **Energy Supplier**, a **Network Operator**, or a **Meter Equipment Manager**.

Leads from industry experts tend to be **reliable**, of **good quality**, with **specific details** about the situation. They often provide photographs to support reports.

Leads may also come from a **member of the public**, tradesperson, or an employee of other **organisations**.

These organisations could include housing associations, local councils, or the police.

These type of reports may **vary in quality** and level of detail but are also a **valuable source** of leads.

REACTIVE ENERGY THEFT LEADS

RETAIL ENERGY CODE



REC Schedule 8 (s5.1)

requires all **Energy Suppliers and Network Operators** to have an appropriate **reporting mechanism** to be able to receive reactive leads.

CrimeStoppers.

XOSERVE

(In Great Britain) reports may also be made anonymously through the **Energy Theft Tip Off Service** (ETTOS), operated by Crimestoppers under the Stay Energy Safe brand. There is a new 2-way contact process which, if the reporter has opted in to, means you can ask them questions or for further information. Learn more**.**

Gas theft leads may also be provided via Xoserve's CMS system as a **Theft of Gas (TOG) contact**. This will be received by the Shipper and passed on to the Supplier to investigate and resolve. Learn more.

REACTIVE ENERGY THEFT LEADS



When a reactive lead or tip-off is received, it is an **obligation to act** on it.

REC Schedule 8 (s3.4)

“Energy Suppliers and Network Parties shall (and shall ensure that their agents shall) act on reports made to them regarding Energy Theft for which they have responsibility… and take the appropriate steps required of them in respect of such Energy Theft…”

PROACTIVE ENERGY THEFT LEADS

RETAIL ENERGY CODE





Proactive leads are generated by analysing data from **internal systems** or **publicly available** sources.

This can help detect anomalies with the meter or consumption that may indicate Energy Theft. The possible anomalies are not limited to the meter readings; could be damage, different serial number etc.

The methods used depend on **consumer types**, **available data** and the organisation's **analytical tools and expertise**. This data analysis identifies meter points that may require further investigation which typically starts with a desktop review, and, if necessary, a site visit.

What data can be used? Examples of data types for detecting energy theft are evolving, especially with **smart meter alerts**. Read more on the next slide.

When creating analysis models or processes, it's important to **account for false positives** and other causes of anomalies to ensure accurate identification of leads.

PROACTIVE LEADS: EXAMPLE OF DATA TYPES

RETAIL ENERGY CODE



Prepayment top ups

- Non-purchase of credit for traditional prepayment or smart meters in prepayment mode
- Credit purchased for gas prepayment meters but not for the electric prepayment meter at the same address
- Minimal credit purchases that only covers the standing charge

Consumption data/meter readings



- Flat consumption year round
- Anomalous consumption patterns where granular consumption data is available
- Lower consumption than typical for the type, size or occupancy of a business or domestic dwelling
- A sudden increase in consumption followed by a sudden and sustained drop to below normal
- Zero consumption but indications the premises are occupied or in use
- Gas consumption recorded but no electricity consumption at the same address

Smart meter alerts



- Specific tamper alerts
- Combinations of alerts in particular sequences
- Smart alerts in conjunction with smart meter reads/consumption data

PROACTIVE LEADS – ELECTRICITY MESSAGES

RETAIL ENERGY CODE

Certain Market Messages or Data Flows can act as reactive leads if they directly report suspected energy theft (e.g. D0237, D0136).

Those listed below can provide indirect information that, when combined with additional data, supports **proactive lead generation**.

- D0001 (**MM00001**) - Request Metering System Investigation
- D0002 (**MM00013**) - Fault Resolution Report or Request for Decision on further Action
- D0003 (**MM00079**) - Half Hourly Advances
- D0004 (**MM00135**) - Notification of Failure to Obtain Reading
- D0008 (**MM00235**) - Meter Advance Reconciliation Report
- D0010 (**MM00257**) - Meter Readings
- D0086 (**MM00004**) - Notification of Change of Supplier Readings
- D0139 (**MM00036**) - Confirmation or Rejection of Energisation Status Change
- D0192 (**MM00102**) - Readings and Settings from a Token or Key Meter
- D0221 (**MM00121**) - Notification of Failure to Install or Energise Metering System
- D0291 (**MM00220**) - Notification of Register Readings on Change of Measurement Class coincident with Change of Supplier

The Site Visit Check Code (J0024/**DI50016**) provides information about the site visit.

Examples of values that may be of use include:

- 05 – Equipment/meter damage
- 06 – Suspected Tampering
- 09 – Consumption detected on de-energised meter
- 15 – Meter Stopped
- 16 – Seals Damaged
- 17 – Seals missing
- 21 – Refused Access
- 22 – Meter Blocked
- 40 – Suspected Energised

PROACTIVE LEADS – GAS MESSAGES

Unlike in electricity, the gas market doesn't send specific Market Messages to alert a Supplier about suspected energy theft.

However, certain data items within existing gas messages can **indirectly signal** that theft might be occurring, especially when these **data points are combined**. These indicators mainly relate to **unusual** or **inconsistent** gas flow information.

This includes gas flows such as:

- **ONJOB** (MM40009)
- **ONUPD** (MM40014)
- **Response** (MM40020)

The Transaction type reason code (DI40174) and Transaction Type reason description can provide information about the visit.

Examples of values that may be of use include:

- **DMGMT – Damaged Meter**
- **FNDAS – Found Asset**
- **MISAS – Missing Asset**
- **SAFTY – Safety and/or Health**
- **TAMPR – Tampering**

PROACTIVE LEADS – GENERAL DATA

RETAIL ENERGY CODE



Publicly available demographic and crime data

Public data such as information on fuel poverty, crime, income, education, employment, and food hygiene, is free to download from government sites. When combined with a supplier's billing and consumption data, it can help identify potential leads more effectively.

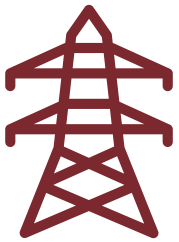


Other departments

Staff across the business who interact with customers or handle billing should receive training on energy-theft indicators. Because they often spot unusual comments, behaviours, or billing issues first, they are well-placed to raise potential Energy Theft Leads.

RECORDING AND REPORTING LEAD SOURCES

The Performance Assurance Catalogue (PARC) details what Energy Theft investigation information must be reported each month to the code manager in the TDIS submissions. A key data item is the **Theft Lead Source**, which identifies the initial source of the investigation. Permitted values include:



T – TRAS generated: Not currently used (no operational TRAS).

S – Supplier generated: Leads from internal supplier processes or data analysis.

C – Crimestoppers: Reports via the Energy Theft Tip-Off Service (ETTOS).



O – Others: Leads from other Suppliers, members of the public, or CMS not linked to field operatives.

M – Third-party meter reader/agent: Visual inspections during meter reading visits.

F – Field agent: Leads from REC Party operatives such as meter installers, debt collectors, or DNO/GT staff.



P – Police: Cases identified during investigations of other crimes by the police.

If you received a tip-off or lead but already have an active investigation in progress, you do not need to change the lead source or raise a new investigation. The lead source should reflect the initial lead source that led you to instigate the investigation.

RETAIL ENERGY CODE

KNOWLEDGE CHECK

KNOWLEDGE CHECK

RETAIL ENERGY CODE

Congratulations, you have completed Module 2!

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

